No.,
Private Library,
of
Dr. Virgil Snyder,
Date Sept. 1 1902

Math
$4.00

512.86
B47
83039

BOOK 512.86.847 c. 1
BIANCHI # LEZIONI SULLA TEORIA
DEI GRUPPI
3 9153 00010965 4

N 8.00
Binding 2.00

LUIGI BIANCHI

PROFESSORE DELLA REGIA UNIVERSITÀ DI PISA

LEZIONI

SULLA

TEORIA DEI GRUPPI DI SOSTITUZIONI

E DELLE

EQUAZIONI ALGEBRICHE SECONDO GALOIS

PISA
ENRICO SPOERRI
Libraio-Editore

1900

513.86
B47

Pisa, Tip. Succ. FF. Nistri.

PREFAZIONE

Colla pubblicazione del presente corso di lezioni, nella forma che una ripetuta esperienza d'insegnamento mi ha consigliato di dargli, ho voluto offrire ai giovani studenti delle Università italiane un libro che li avvii allo studio di una fra le più importanti teorie dell'odierna matematica e li prepari alla lettura delle opere maggiori e più complete, ove trovansi interamente svolti, in tutte le loro conseguenze, i principii dovuti all'immortale Galois e dimostrata tutta la loro fecondità ed efficacia.

Il lettore già esperto nella materia non cerchi nella presente opera novità di risultati, o di metodi. Sarà raggiunto il mio scopo, se si giudicherà opportuna la scelta degli argomenti e giusta l'estensione data, nella trattazione, a ciascuno di essi: se si troverà che alcune dimostrazioni risultano semplificate, altre condotte con mezzi più elementari, quali richiedeva la natura del libro, destinato a giovani appena in possesso delle consuete nozioni d'algebra complementare.

Le opere che maggiormente ho posto a contributo, nel redigere le presenti lezioni, sono le seguenti:

Jordan . — *Traité des substitutions et des équations algébriques.* (Paris, G. Villars, 1870).

Netto. . — *Substitutionentheorie und ihre Anwendungen auf die Algebra.* (Leipzig, Teubner, 1882).

Klein . . — *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade.* (Leipzig, Teubner, 1884).

Weber . — *Lehrbuch der Algebra.* (Braunschweig, Vieweg, 1895).

Cito ancora, per raccomandarne vivamente lo studio:

BURNSIDE — *Theory of groups of finite order.* (Cambridge, University Press, 1897).

Questo ottimo libro contiene una teoria completa dei gruppi finiti, che giunge fino ai più recenti risultati; ma fu da me conosciuto troppo tardi per poterne trarre profitto.

Avverto in fine che per lo scopo puramente didattico dell'opera mi sono ritenuto dispensato dall'obbligo di citazioni storiche, che il lettore, desideroso di conoscere le fonti, troverà largamente sparse nelle opere sopra ricordate.

Pisa, luglio 1899.

L. BIANCHI.

PARTE PRIMA

Teoria dei gruppi di sostituzioni

Capitolo I.

Sostituzioni e loro composizione. — Periodo di una sostituzione. — Sostituzioni circolari. — Sostituzioni pari e dispari. — Sostituzioni simili e permutabili. — Gruppi di sostituzioni. — Teorema fondamentale e corollarii. — Gruppo alterno. — Gruppi transitivi ed intransitivi. — Limite superiore del grado di transitività. — Gruppi imprimitivi.

§. 1. — Consideriamo un numero qualunque n di oggetti, che rappresentiamo con n lettere

$$x_1, x_2, x_3 \ldots . x_n .$$

Se con

$$i_1, i_2, i_3 \ldots i_n$$

indichiamo ancora i numeri 1, 2, 3... n, in altro ordine, il succedersi degli n oggetti nell'ordine

$$x_{i_1}, x_{i_2} \ldots x_{i_n}$$

dicesi una permutazione degli oggetti stessi.

Il numero delle permutazioni distinte è dato, come è noto, dal fattoriale

$$\pi(n) = 1 . 2 . 3 \ldots n .$$

Chiamasi *sostituzione* l'operazione colla quale si passa da una permutazione ad un'altra. Si rappresenta la sostituzione scrivendo in una prima linea orizzontale la permutazione da cui si parte, in una seconda orizzontale superiore la permutazione a cui si arriva. Così p. e., se partiamo dalla permutazione

$$x_1 \, x_2 \, x_3 \ldots x_n$$

ed arriviamo alla permutazione

$$x_{i_1}\, x_{i_2}\, x_{i_3} \ldots x_{i_n}\ ,$$

scriveremo la sostituzione col simbolo

$$\begin{pmatrix} x_{i_1}\, x_{i_2}\, x_{i_3} \ldots . x_{i_n} \\ x_1\ x_2\ x_3 \ldots . x_n \end{pmatrix}.$$

Diciamo subito che due sostituzioni si riguardano come identiche quando a ciascuno degli n oggetti sostituiscono un medesimo oggetto; così p. e. sono identiche le due sostituzioni

$$\begin{pmatrix} x_3\, x_1\, x_4\, x_2 \\ x_1\, x_2\, x_3\, x_4 \end{pmatrix}\ ,\quad \begin{pmatrix} x_1\, x_2\, x_3\, x_4 \\ x_2\, x_4\, x_1\, x_3 \end{pmatrix}.$$

Ne segue che, nel rappresentare una sostituzione, possiamo prendere come permutazione iniziale una qualunque permutazione fissa, p. e. la permutazione principale

$$x_1\, x_2\, x_3 \ldots x_n\,.$$

Se indichiamo quindi con

$$\sum\nolimits_1\ ,\ \sum\nolimits_2\ ,\ \sum\nolimits_3 \ldots \sum\nolimits_{\pi\,(n)}$$

le $\pi\,(n)$ permutazioni distinte, altrettante saranno le sostituzioni distinte da indicarsi coi simboli:

$$\begin{pmatrix} \sum\nolimits_1 \\ \sum\nolimits_1 \end{pmatrix}\ ,\ \begin{pmatrix} \sum\nolimits_2 \\ \sum\nolimits_1 \end{pmatrix}\ ,\ \begin{pmatrix} \sum\nolimits_3 \\ \sum\nolimits_1 \end{pmatrix} \ldots .\ \begin{pmatrix} \sum\nolimits_{\pi\,(n)} \\ \sum\nolimits_1 \end{pmatrix}.$$

Fra queste la prima, che lascia ogni lettera al proprio posto, dicesi la *sostituzione identica* o *l'identità*. Spesso rappresenteremo le sostituzioni con semplici lettere

$$\mathrm{S}\ ,\ \mathrm{T} \ldots ..$$

e in particolare l'identità col simbolo 1.

Se S, T sono due qualunque sostituzioni, possiamo considerare una terza sostituzione U che nasce eseguendo S, T successivamente in un ordine determinato p. e. prima S, poi T. Per ottenere la U basterà partire ad esempio dalla permutazione principale Σ_1 ed operare su questa mediante la S, ciò che condurrà alla nuova permutazione Σ_2; indi, ope-

rando sulla permutazione Σ_2 la sostituzione T, si otterrà una nuova permutazione Σ_3 e la sostituzione U sarà data da

$$U = \begin{pmatrix} \Sigma_3 \\ \Sigma_1 \end{pmatrix}.$$

Questa sostituzione U dicesi *composta* delle due S, T od anche il *prodotto* di queste sostituzioni e si scrive simbolicamente

$$U = S\,T,$$

ponendo a sinistra la sostituzione eseguita prima. È necessario fissare la convenzione fondamentale riguardo al significato della scrittura S T perchè, alterando l'ordine delle sostituzioni componenti, cangia in generale la sostituzione composta. Così p. e. se si pone

$$S = \begin{pmatrix} x_3 & x_4 & x_2 & x_1 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}, \quad T = \begin{pmatrix} x_4 & x_3 & x_2 & x_1 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix},$$

si avrà

$$S\,T = \begin{pmatrix} x_2 & x_1 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}, \quad T\,S = \begin{pmatrix} x_1 & x_2 & x_4 & x_3 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}.$$

Quando due sostituzioni S, T soddisfano alla condizione

$$S\,T = T\,S,$$

si dicono fra loro *permutabili.*

Stabilito il significato del prodotto di due sostituzioni, resta naturalmente fissato anche il significato del prodotto di più successive sostituzioni $S_1, S_2, S_3 \ldots S_m$. Intendiamo per sostituzione composta U, che scriviamo

$$U = S_1 . S_2 . S_3 \ldots S_m, \tag{1}$$

quella che nasce componendo prima S_1 con S_2, indi la sostituzione composta $S_1 S_2$ con S_3, questa alla sua volta con S_4 e così via. La formola (1) sta dunque propriamente per l'altra

$$U = \big((S_1\ S_2)\ .\ S_3)\big)\ S_4 \ldots .$$

In un prodotto di più sostituzioni non è lecito in generale, come già si è avvertito, invertire due o più fattori, cioè non vale la legge

commutativa dei prodotti di ordinarie quantità. Ma un'altra importante legge, che vale per gli ordinarii prodotti, quella *associativa*, sussiste inalterata pei prodotti di sostituzioni; cioè, fissate ad arbitrio nel prodotto più sostituzioni successive S_i, $S_{i+1} \ldots S_{i+v}$, potremo, senza alterare il prodotto, sostituire al loro insieme il loro prodotto eseguito. Per dimostrare l'asserita proprietà basterà provare che nel prodotto di tre fattori vale la legge *elementare* associativa espressa dalla formola

$$(2) \qquad (S_1 \,.\, S_2) \,.\, S_3 = S_1 \,(S_2 \,.\, S_3).$$

Verifichiamo che le sostituzioni dei due membri sono in effetto identiche, osservando che sopra una lettera qualunque x_i hanno il medesimo effetto. Supponiamo infatti che la S_1 porti x_i in x_k, la S_2 porti x_k in x_l e in fine la S_3 porti x_l in x_m, sicchè la sostituzione a sinistra in (2) porta x_i in x_m. Il prodotto $S_2 S_3$ porta x_k in x_m e per ciò anche la sostituzione a destra in (2) porta x_i in x_m.

Terminiamo queste considerazioni preliminari, osservando che se due sostituzioni A, B sono identiche e C è una terza sostituzione qualunque, anche i risultati che si ottengono componendo sia A, sia B con C, nel medesimo ordine, sono identici, cioè da

$$A = B$$

segue tanto

$$AC = BC,$$

quanto

$$CA = CB.$$

Viceversa da una qualunque di queste seconde eguaglianze segue la prima.

§. 2. — Quando tutte le m sostituzioni componenti di un prodotto

$$S_1, S_2 \ldots S_m$$

sono uguali fra loro e ad una medesima sostituzione S, il prodotto stesso dicesi la potenza m^{esima} di S e si indica col simbolo S^m. A causa della legge associativa, è chiaro che due potenze di una medesima sostituzione S, moltiplicate fra loro, danno una potenza di S il cui esponente è la somma degli esponenti delle potenze componenti; in simboli si ha

$$(3) \qquad S^m \,.\, S^p = S^{m+p},$$

onde segue in particolare che due potenze di una medesima sostituzione S sono sempre fra loro permutabili.

La notazione S^m ha per ora soltanto un significato quando l'esponente m sia intero e positivo. Ma conviene, con opportune convenzioni, considerare anche potenze di S con esponente intero negativo o nullo. Ciò si ottiene considerando insieme ad S la sua sostituzione *inversa* S', quella cioè che, riportando le lettere spostate da S nei posti che prima occupavano, dà luogo, per composizione con S, alla identità. Conveniamo di considerare questa inversa S' di S come potenza di S con esponente -1, scriviamo cioè

$$S' = S^{-1};$$

ed allora, essendo $-n$ un intero qualunque negativo, definiremo la potenza S^{-n} di S come potenza n^{ma} di $S' = S^{-1}$; cioè converremo che sia

$$S^{-n} = (S^{-1})^n.$$

Dopo ciò la formola (3) varrà per esponenti interi (non nulli) positivi o negativi, purchè non sia $m + p = 0$, nel qual caso si avrà invece

$$S^m . S^p = S^m . S^{-m} = 1.$$

Per togliere quest'ultima restrizione alla validità della (3) basterà fare l'ulteriore convenzione che assegna alla potenza S^0 il significato dell'identità; e così la (3) sussisterà in tutti i casi.

Consideriamo ora la serie infinita nei due sensi delle potenze di S:

$$(4) \qquad \ldots\ldots S^{-3}, S^{-2}, S^{-1}, S^0 = 1, S, S^2, S^3 \ldots.$$

Poichè il numero delle sostituzioni diverse è finito $= \pi(n)$, se percorriamo in (4) ad esempio la serie ascendente, da un certo punto in poi non incontreremo più nuove sostituzioni, ma si ripeteranno necessariamente le precedenti. Ora si vede subito che la prima sostituzione ripetuta sarà l'identità, poichè da

$$S^{\alpha+\beta} = S^\alpha$$

segue, moltiplicando per $S^{-\alpha}$

$$S^\beta = 1.$$

Il più piccolo esponente β *(intero) positivo, pel quale risulta* $S^\beta = 1$, *dicesi il periodo (o l'ordine) della sostituzione* S.

Se β è il periodo di S, le β potenze

$$(5) \qquad 1, S, S^2, \ldots S^{\beta-1}$$

sono tutte fra loro distinte, ma ogni altra potenza S^m è uguale ad una delle (5). E invero, se r indica il minimo resto positivo (mod β) del numero m (positivo o negativo), si avrà

$$m = q\beta + r$$

con q intero e quindi

$$S^m = S^{q\beta} \,.\, S^r = (S^\beta)^q \,.\, S^r = S^r \,.$$

Deduciamo quindi il teorema:

Perchè due potenze S^m, $S^{m'}$ *di* S *siano fra loro eguali è necessario e sufficiente che gli esponenti* m, m' *siano congrui rispetto al periodo* β; *in simboli*

$$m \equiv m' \pmod{\beta} \,.$$

In particolare perchè si abbia $S^m = 1$ sarà necessario e sufficiente che sia m multiplo del periodo β.

Si può ora facilmente risolvere la questione di determinare il periodo β' di ogni potenza S^α di S. Sarà questo il minimo valore intero e positivo che si potrà dare a β' in guisa da soddisfare la congruenza

$$\alpha\beta' \equiv 0 \pmod{\beta} \,;$$

Indicando dunque con ε il massimo comun divisore di α, β, avremo

$$\beta' = \frac{\beta}{\varepsilon} \,.$$

In particolare il periodo di S^α sarà ancora β se α è primo con β; e vi saranno per ciò tante potenze di S a periodo β quanti numeri primi con β si trovano nelle serie 1, 2, 3, ... $\beta - 1$ cioè, nella ordinaria notazione della teoria dei numeri, precisamente $\varphi(\beta)$.

§. 3. — Una sostituzione S dicesi *circolare* o *ciclica* quando le lettere che essa sposta possono ordinarsi in guisa che la S porti ciascuna lettera nella seguente e l'ultima nella prima. Così p. e. la sostituzione

$$S = \begin{pmatrix} x_3 & x_1 & x_4 & x_2 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}$$

opera ciclicamente sulla permutazione

$$x_1 \; x_3 \; x_4 \; x_2$$

ed è per ciò ciclica. Una sostituzione ciclica è definita, appena data la permutazione su cui opera circolarmente, e si scrive più brevemente racchiudendo fra parentesi questa permutazione. Così la sostituzione ciclica precedente si scriverà

$$S = (x_1 \; x_3 \; x_4 \; x_2).$$

Se n sono le lettere sulla quale S opera ciclicamente, potremo scrivere così la S in n modi diversi, facendo cominciare la permutazione da una qualunque delle sue lettere. Il periodo di una sostituzione ciclica su n lettere è evidentemente eguale ad n. Dimostriamo ora che:

Qualunque sostituzione può decomporsi nel prodotto di più sostituzioni cicliche, operanti su lettere diverse.

Sia infatti x_{i_1} una qualunque delle lettere e supponiamo che S porti x_{i_1} in x_{i_2}, la x_{i_2} in x_{i_3} e così via. Nella successione di lettere

$$x_{i_1} \; x_{i_2} \; x_{i_3} \ldots\ldots \tag{6}$$

la prima lettera ripetuta sarà certamente la x_{i_1} poichè se le lettere

$$x_{i_r} \quad x_{i_k}$$

nella successione sono identiche, identiche saranno pure le due precedenti

$$x_{i_{r-1}} \; , \quad x_{i_{k-1}} \, ,$$

che la S porta nella medesima $x_{i_r} = x_{i_k}$.

Poniamo che la successione (6) contenga le sole r lettere

$$x_{i_1} \; x_{i_2} \ldots x_{i_r} \, ,$$

sulle quali adunque la S produca lo stesso effetto che la sostituzione ciclica

$$C_1 = (x_{i_1} \; x_{i_2} \ldots x_{i_r}).$$

Se non vi sono altre lettere spostate da S, la S è senz'altro la sostituzione circolare C_1. Altrimenti si prenda un'altra lettera x_{k_1} e si proceda su questa nel medesimo modo costruendo il ciclo corrispondente

$$C_2 = (x_{k_1} \; x_{k_2} \ldots x_{k_s}).$$

Così continuando, decomporremo appunto S nel prodotto di più sostituzioni cicliche:

$$S = C_1 C_2 \ldots C_i \; ; \tag{7}$$

e si noti che queste sostituzioni circolari componenti di S, operando ciascuna su lettere diverse, sono due a due permutabili. La decomposizione (7) di una sostituzione S in prodotto di sostituzioni circolari è quella che torna più spesso utile. Intanto possiamo subito dedurne il modo di calcolare il periodo di S, senza costruirne effettivamente le successive potenze, col teorema:

Il periodo β *di una sostituzione* S *è il minimo multiplo comune degli ordini (o periodi) dei cicli* $C_1, C_2 \ldots C_i$ *in cui* S *si decompone.*

E infatti se si ha

$$S^\beta = (C_1 C_2 \ldots C_i)^\beta = 1 \, ,$$

a causa della permutabilità dei cicli, potremo scrivere

$$C_1^\beta \, . \, C_2^\beta \ldots C_i^\beta = 1$$

e, poichè i singoli cicli operano su lettere differenti, si dovrà avere separatamente

$$C_1^\beta = 1 \; , \; C_2^\beta = 1 \ldots C_i^\beta = 1 \, .$$

Ne segue che β è certamente multiplo dei singoli periodi dei cicli. D'altronde, se β il minimo multiplo comune di questi periodi, si ha inversamente

$$S^\beta = 1 \, ,$$

ciò che dimostra la proposizione.

§. 4. — Dicesi *trasposizione* una sostituzione ciclica su due lettere. È facile ora vedere che: *Qualunque sostituzione può scindersi nel prodotto di più trasposizioni.* Per passare infatti da una permutazione ad un'altra si può cominciare, eseguendo una trasposizione, dal portare una lettera della prima al posto che deve occupare nella seconda, dopo di che rimarrà da procedere nel medesimo modo sulle rimanenti lettere. Si arriva al medesimo risultato osservando che ogni sostituzione circolare d'ordine r si compone di $r-1$ trasposizioni; così p. e.

$$(x_1 \, x_2 \, x_3 \ldots x_r) = (x_1 \, x_2) \; (x_1 \, x_3) \ldots (x_1 \, x_r) \, .$$

D'altronde ogni sostituzione si decompone, come si è visto, in sostituzioni circolari. È da osservarsi che decomponendo una sostituzione nel prodotto di trasposizioni, queste non opereranno in generale su lettere diverse; anzi, a meno che la sostituzione non abbia il periodo 2, vi sarà necessariamente qualche lettera comune a trasposizioni diverse.

La decomposizione di una sostituzione S nel prodotto di trasposizioni si può eseguire in modi diversi; ma, in qualunque modo si eseguisca, dimostriamo che il numero delle trasposizioni in cui S si decompone è sempre pari o sempre dispari. Per dimostrarlo, scindiamo S in sostituzioni circolari, ove espressamente avvertiamo che valutiamo in S come cicli anche quelli composti di una sola lettera, di quelle lettere cioè che S non sposta, e cominciamo dal dimostrare che: *Se si moltiplica* S, *a destra o a sinistra, per una trasposizione* T, *il numero dei cicli in* ST (*o* TS) *aumenterà o diminuirà, rispetto a quello di* S, *precisamente di un'unità.*

Distinguiamo per ciò due casi secondo che le due lettere della trasposizione T appartengono ad un medesimo ciclo C o a cicli diversi C, C' in S. Nel primo caso potremo evidentemente supporre che la prima lettera di C appartenga a T; sia dunque

$$C = (x_1\, x_2 \ldots x_{r-1}\, x_r\, x_{r+1} \ldots x_m)$$
$$T = (x_1\, x_r).$$

Essendo T permutabile con tutti gli altri cicli di S, ed avendosi

$$CT = (x_1\, x_2 \ldots x_{r-1})\ (x_r\, x_{r+1} \ldots x_m),$$

ne risulta appunto che in ST all'unico ciclo C ne vengono sostituiti 2 [1]).

Nel secondo caso potremo supporre

$$C = (x_1\, x_2 \ldots x_r)$$
$$C' = (y_1\, y_2 \ldots y_s)$$
$$T = (x_1\, y_1)$$

e poichè T è permutabile con tutti gli altri cicli di S, oltre C, C', mentre si ha

$$CC'T = (x_1\, x_2 \ldots x_r\, y_1\, y_2 \ldots y_s),$$

---

[1]) Si osservi peraltro che uno di questi cicli può constare di una sola lettera; ciò avviene per $r = 2$, o per $r = m$.

i due cicli C, C′ di S si sono riuniti in ST in un solo, ciò che dimostra il nostro lemma.

Ora essendo

$$x_1, x_2 \ldots x_n$$

le lettere, supponiamo che la S, decomposta in cicli, presenti k cicli, computando come sopra anche i cicli di una sola lettera e sia d'altra parte decomposta nel prodotto di m trasposizioni:

$$S = T_1 T_2 \ldots T_m$$

avremo

$$S T_m T_{m-1} \ldots T_2 T_1 = 1$$

e poichè l'identità consta di n cicli (del 1.° ordine) e moltiplicando per una trasposizione ogni volta il numero dei cicli aumenta o diminuisce di un'unità, ne deduciamo

$$k + m \equiv n \pmod 2,$$

cioè

$$m \equiv n + k \pmod 2.$$

Decomponendo S in un altro prodotto di m' trasposizioni, sarà dunque necessariamente

$$m' \equiv m \pmod 2,$$

come si era asserito.

Questi risultati danno luogo alla classificazione delle sostituzioni in *pari* e *dispari*, secondo che si compongono di un numero pari o dispari di trasposizioni. È chiaro che un prodotto di più sostituzioni è pari o dispari, secondo che vi è un numero pari o dispari di sostituzioni dispari componenti.

Abbiamo osservato sopra che una sostituzione ciclica d'ordine r equivale al prodotto di $r - 1$ trasposizioni. Se la sostituzione S si compone di k cicli contenenti rispettivamente

$$n_1, n_2, \ldots . n_k$$

lettere, essa sarà pari o dispari secondo che il numero

$$q = \sum (n_i - 1) = n_1 + n_2 + \ldots + n_k - k$$

sarà pari o dispari e per l'applicazione di questo criterio sarà evidentemente indifferente comprendere o no fra i cicli quelli di una sola lettera.

§. 5. — Siano S, T due sostituzioni qualunque; costruiamo la sostituzione

$$S_1 = T^{-1} S T.$$

Questa dicesi la *trasformata di* S *per mezzo della* T. Siccome si ha inversamente

$$S = T S_1 T^{-1} = (T^{-1})^{-1} S_1 T^{-1},$$

si vede che S è, alla sua volta, trasformata di S_1 per mezzo della inversa T^{-1} di T.

Supponiamo S decomposta in cicli e sia

$$C = (x_1 x_2 x_3 \ldots x_r)$$

un suo ciclo; indichiamo con $y_1, y_2, \ldots y_r$ le lettere in cui la sostituzione trasformatrice T trasporta rispettivamente $x_1, x_2 \ldots x_r$. Il ciclo della trasformata $S_1 = T^{-1} S T$, cui appartiene y_1, sarà precisamente

$$C_1 = (y_1 y_2 \ldots y_r),$$

onde risulta la regola seguente:

Per ottenere la trasformata della S *per mezzo della* T *basta decomporre* S *in cicli ed eseguire sulle lettere di ciascun ciclo di* S *la sostituzione* T.

È chiaro quindi che $S_1 = T^{-1} S T$ ed S hanno il medesimo numero di cicli e nei cicli corrispondenti il medesimo numero di lettere. Viceversa se due sostituzioni S, S_1 si decompongono in un egual numero di cicli di ordini rispettivamente eguali, indicando con T una sostituzione che trasporti ogni lettera di un ciclo di S nella corrispondente del corrispondente ciclo di S_1, si avrà

$$S_1 = T^{-1} S T,$$

cioè la S_1 sarà una trasformata della S.

Due sostituzioni trasformate l'una dell'altra diconsi anche *simili* fra loro. Esse possono farsi coincidere, cangiando soltanto la denominazione delle lettere.

Notiamo ora le proposizioni seguenti d'immediata dimostrazione:

1.ª *Se* S, S′ *sono due sostituzioni qualunque, i due prodotti*

$$S S' \quad , \quad S' S$$

sono simili.

E infatti si ha

$$S' S = S^{-1} (S S') S .$$

2.ª *La trasformata di un prodotto è eguale al prodotto delle trasformate, restando la medesima la sostituzione trasformatrice.*

Si ha invero, a causa della legge associativa

$$(T^{-1} S_1 T) (T^{-1} S_2 T) \ldots (T^{-1} S_m T) = T^{-1} (S_1 S_2 \ldots S_m) T.$$

In particolare si osservi che

$$(T^{-1} S T)^m = T^{-1} S^m T.$$

§. 6. — Stabilite queste prime nozioni sulle sostituzioni, arriviamo all'importante e fondamentale concetto di *gruppo di sostituzioni*. Un sistema di un numero qualunque di sostituzioni sopra n lettere dicesi un *gruppo* se il prodotto di due sostituzioni qualsiasi (differenti od anche eguali) nel sistema appartiene nuovamente al sistema stesso [1]). In particolare si osservi che un gruppo, insieme ad ogni sua sostituzione S, ne contiene anche tutte le potenze e perciò anche l'identità.

Il concetto di gruppo, nato dapprima appunto dalla teoria delle sostituzioni, ha acquistato successivamente nelle matematiche un'estensione ed una importanza sempre maggiori. Esso è applicabile in tutti quei casi ove si ha una serie finita od infinita, discontinua o continua, di *operazioni*, di qualunque natura esse siano, purchè esista una legge di composizione, secondo la quale due operazioni qualsiasi A, B della serie si compongano in una terza determinata

$$C = A B$$

e valga la legge associativa insieme alle altre leggi elementari indicate alla fine del n.° 1. Come esempî di operazioni di questa specie, citiamo i movimenti dello spazio o più in generale le trasformazioni projettive, che possiamo ancora riguardare come *sostituzioni* sopra oggetti, p. e. sui punti dello spazio; soltanto il numero degli oggetti invece di essere finito è qui infinito, anzi forma una continuità di oggetti. I gruppi generali

---

[1]) Per denotare un tale sistema di sostituzioni CAUCHY adoperava il termine *sistema coniugato di sostituzioni;* la denominazione più breve, ed ora universalmente adottata, di *gruppo* proviene da GALOIS.

di operazioni possono essere finiti o infiniti, secondo che le loro operazioni sono in numero finito od infinito. Ulteriormente i gruppi infiniti si dividono in gruppi *discontinui* e gruppi *continui*. Nei primi le operazioni del gruppo formano una serie discreta per quanto infinita, nei secondi le operazioni stesse del gruppo sono suscettibili di variare con continuità, contenendo dei parametri arbitrarî.

Arrestandoci ai gruppi finiti di operazioni (chè di questi soli tratteremo nel presente corso), diciamo subito che il loro studio si riduce essenzialmente a quello di un gruppo di sostituzioni sopra lettere, come dimostreremo prossimamente (§. 15). Noi parleremo quindi soltanto di gruppi di sostituzioni, ma le teorie che svolgeremo conserveranno la loro validità nel caso generale di gruppi finiti di operazioni.

Dicesi *ordine* di un gruppo di sostituzioni il numero delle sostituzioni in esso contenute. Il più semplice esempio di un gruppo si ottiene formando tutte le potenze di una medesima sostituzione S; se β è il periodo di S, le β sostituzioni

$$1, S, S^2, \ldots S^{\beta-1}$$

formano appunto un gruppo d'ordine β.

Un tale gruppo dicesi un gruppo ciclico.

Un altro esempio di gruppo l'abbiamo nella totalità delle $\pi(n)$ sostituzioni sopra n lettere; questo dicesi il *gruppo totale* su n lettere o *gruppo simmetrico*.

Ancora consideriamo tutte le sostituzioni *pari* su n lettere. Esse formano evidentemente un gruppo; questo dicesi il *gruppo alterno* o *gruppo semisimmetrico*.

Il suo ordine è uguale a

$$\frac{1}{2}\pi(n) = 3 \,.\, 4 \,.\, 5 \ldots n,$$

come si rileva subito dall'osservare che moltiplicando tutte le $\pi(n)$ sostituzioni da una medesima parte per una sostituzione dispari, p. e. una trasposizione, si ottengono ancora tutte le $\pi(n)$ sostituzioni, ma le pari si cangiano in dispari e viceversa.

Dicesi *sottogruppo* di un gruppo G ogni gruppo Γ le cui sostituzioni appartengano tutte a G. Così se S è una sostituzione di G a periodo β il gruppo ciclico

$$\Gamma_\beta = [1, S, S^2, \ldots S^{\beta-1}]$$

è un sottogruppo di G. Medesimamente il gruppo alterno è un sottogruppo del gruppo totale.

§. 7. — Sia G_m un gruppo d'ordine m, Γ_n un suo sottogruppo d'ordine n. Possiamo distribuire le sostituzioni del gruppo, rispetto a quelle del sottogruppo, secondo una certa legge fondamentale, alla quale in seguito dovremo sempre ricorrere. In particolare stabiliremo così il teorema fondamentale:

L'ordine n del sottogruppo Γ è sempre un divisore dell'ordine m del gruppo G.

Indichiamo con

$$a) \qquad \gamma_1 = 1, \gamma_2, \gamma_3 \ldots \gamma_n$$

le sostituzioni di Γ e sia t_2 una sostituzione di G fuori di Γ [1]). Se moltiplichiamo tutte le sostituzioni di Γ da una medesima parte, p. e. a destra, per t_2 e formiamo le m sostituzioni

$$b) \qquad \gamma_1 t_2, \gamma_2 t_2, \gamma_3 t_2, \ldots \gamma_n t_2,$$

queste, come prodotti di sostituzioni di G, appartengono certamente tutte a G. Esse sono inoltre tutte diverse fra loro e dalle precedenti. E infatti se due delle b) fossero eguali, p. e. si avesse

$$\gamma_i t_2 = \gamma_j t_2,$$

moltiplicando a destra per t_2^{-1} (§. 1) risulterebbe

$$\gamma_i = \gamma_j,$$

ciò che è assurdo se $i \neq j$. Se poi una delle b) eguagliasse una delle a) p. e.

$$\gamma_i t_2 = \gamma_j,$$

moltiplicando a sinistra per γ_i^{-1}, avremmo

$$t_2 = \gamma_i^{-1} \gamma_j .$$

Ma la sostituzione a destra, come prodotto di due sostituzioni del gruppo Γ, è in Γ, ciò che è contrario all'ipotesi fatta sopra t_2. Dunque G contiene almeno le $2n$ sostituzioni distinte a) b) e, se non ne con-

---

[1]) Se non esistesse una tale sostituzione Γ coinciderebbe con G e si avrebbe, conformemente al teorema enunciato, $m = n$.

tiene altre, il suo ordine è dato da $m = 2n$ ed è quindi multiplo di n, come è asserito nel teorema. Se invece $m > 2n$, sia t_3 una nuova sostituzione di G, che non sia nè nella serie *a*) nè in *b*), e formiamo le n sostituzioni di G

$$c) \qquad \gamma_1 t_3, \gamma_2 t_3, \ldots \gamma_n t_3 .$$

Con ragionamento affatto analogo a quello sopra esposto si vede che due delle *c*) non possono essere eguali, nè può una sostituzione *c*) eguagliare una *a*) o una *b*). Le $3n$ sostituzioni di G contenute nelle serie *a*) *b*) *c*) sono dunque tutte distinte e per ciò, se esse esauriscono il gruppo G, si avrà, conformemente al teorema,

$$m = 3n .$$

Continuando nel medesimo modo, è chiaro che ogniqualvolta, dopo avere costruito un certo numero di orizzontali come *a*) *b*) *c*) ..., queste non esauriscono G, si potrà costruire una nuova orizzontale contenente n sostituzioni di G tutte diverse fra loro e dalle precedenti. Ma poichè il numero m delle sostituzioni di G è finito, sarà pure finito il numero q di queste orizzontali ed avremo quindi

$$m = qn ,$$

ciò che dimostra il teorema. Inoltre vediamo, ed è questo un risultato fondamentale, che tutte le sostituzioni del gruppo G potranno distribuirsi, rispetto al sottogruppo Γ, nel quadro

$$(A) \quad \left\{ \begin{array}{l} \gamma_1, \gamma_2, \gamma_3 \ldots \gamma_n \\ \gamma_1 t_2, \gamma_2 t_2, \gamma_3 t_2 \ldots \gamma_n t_2 \\ \gamma_1 t_3, \gamma_2 t_3, \gamma_3 t_3 \ldots \gamma_n t_3 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \gamma_1 t_q, \gamma_2 t_q, \gamma_3 t_q \ldots \gamma_n t_q , \end{array} \right.$$

contenente q orizzontali di n sostituzioni ciascuna. Si osservi che le sostituzioni della prima orizzontale sono quelle del sottogruppo Γ; ma quelle di un'altra orizzontale non formano più, in generale, gruppo fra loro.

Il quoziente $q = \frac{m}{n}$, *che si ottiene dividendo l'ordine* m *del gruppo* G *per l'ordine* n *del sottogruppo* Γ, *dicesi l'indice del sottogruppo* Γ *nel gruppo* G.

Spesso scriveremo più compendiosamente il quadro (A) così:

$$G = (\Gamma,\ \Gamma t_2, \Gamma t_3, \ldots \Gamma t_q).$$

Abbiamo formato il quadro (A), ponendo le sostituzioni *moltiplicatrici* $t_1 = 1, t_2, t_3 \ldots t_q$ a destra. Si può evidentemente formare un quadro analogo con q sostituzioni moltiplicatrici

$$\tau_1 = 1,\ \tau_2,\ \tau_3 \ldots \tau_q$$

a sinistra, ottenendo il nuovo quadro

$$(A^*) \left\{ \begin{array}{l} \gamma_1, \gamma_2, \gamma_3 \ldots \gamma_n \\ \tau_2 \gamma_1, \tau_2 \gamma_2, \tau_2 \gamma_3 \ldots \tau_2 \gamma_n \\ \tau_3 \gamma_1, \tau_3 \gamma_2, \tau_3 \gamma_3 \ldots \tau_3 \gamma_n \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \tau_q \gamma_1, \tau_q \gamma_2, \tau_q \gamma_3 \ldots \tau_q \gamma_n, \end{array} \right.$$

che scriveremo anche

$$G = (\Gamma, \tau_2 \Gamma, \tau_3 \Gamma, \ldots \tau_q \Gamma).$$

Dal teorema fondamentale dimostrato seguono corollarii importanti che basta enunciare:

1.° *L'ordine di un gruppo di sostituzioni sopra n lettere è sempre un divisore di* π (n).

2.° *Il periodo di una sostituzione* S *di un gruppo* G *è un divisore dell'ordine del gruppo.*

Dalla definizione stessa di gruppo seguono poi le proposizioni seguenti d'immediata dimostrazione:

1.ª *Le sostituzioni comuni a due gruppi* G, G' *formano un sottogruppo* Γ *comune a* G, G'.

2.ª *Se fra le sostituzioni di un gruppo* G *si conservano solo quelle che non spostano determinate lettere* $x_{i_1}, x_{i_2} \ldots x_{i_r}$, *si ottiene un sottogruppo di* G. Ciò risulta dall'osservare che se due sostituzioni g_1, g_2 di G non spostano $x_{i_1} x_{i_2} \ldots, x_{i_r}$, nemmeno il prodotto $g_1 g_2$ sposta queste lettere.

3.ª *Quelle sostituzioni di un gruppo* G, *che sono permutabili con una medesima sostituzione* T *(in* G *o fuori di* G), *formano un sottogruppo.*

E invero, se g_1, g_2 sono due sostituzioni di G permutabili con T, da

$$g_1 T = T g_1\ ,\ g_2 T = T g_2$$

segue

$$(g_1 g_2) \mathrm{T} = g_1 \mathrm{T} g_2 = \mathrm{T} (g_1 g_2) .$$

§. 8. — Il gruppo alterno su n lettere è un sottogruppo d'indice 2 nel gruppo totale. Ora importa dimostrare il teorema:

Nel gruppo totale G *sopra n lettere non è contenuto alcun altro sottogruppo d'indice* 2 *all'infuori del gruppo alterno.*

Sia Γ un sottogruppo d'ordine $\frac{1}{2} \pi (n)$ del gruppo totale e siano

$$\gamma_1, \gamma_2, \ldots \gamma_{\frac{\pi(n)}{2}}$$

le sue sostituzioni. Indicando con T una *qualunque* sostituzione di G fuori di Γ, possiamo distribuire tutte le $\pi (n)$ sostituzioni nel quadro (A) di due orizzontali:

$$\mathrm{G} = \left| \begin{matrix} \gamma_1, \gamma_2, \ldots \gamma_{\frac{1}{2}\pi(n)} \\ \gamma_1 \mathrm{T}, \gamma_2 \mathrm{T}, \ldots \gamma_{\frac{1}{2}\pi(n)} \mathrm{T} \end{matrix} \right.$$

La sostituzione T^2 è certo fra queste $\pi (n)$, ma non può appartenere alla seconda orizzontale poichè, se fosse

$$\mathrm{T}^2 = \gamma_i \mathrm{T} ,$$

ne risulterebbe $\mathrm{T} = \gamma$, contro l'ipotesi che T non sia in Γ. Dunque T^2 e quindi tutte le potenze pari di T

$$\mathrm{T}^4 , \mathrm{T}^6 \ldots$$

sono in Γ, onde segue che le potenze con esponenti dispari di T sono, come T, fuori di Γ. Ma, se β è il periodo di T, la $\mathrm{T}^\beta = 1$ è certo in Γ, per cui β è necessariamente pari. Dunque intanto il sottogruppo Γ supposto dovrà contenere tutte le sostituzioni a periodo impari, in particolare quindi tutte le sostituzioni circolari su tre lettere. Il teorema enunciato sarà quindi dimostrato se proviamo che sussiste l'altro:

Se un gruppo di sostituzioni sopra n lettere contiene tutte le sostituzioni circolari su tre lettere, esso coincide col gruppo alterno o col gruppo totale.

Ora osserviamo che qualunque prodotto di *due* trasposizioni o è una sostituzione circolare su tre lettere, o un prodotto di due tali sostitu-

zioni, secondo che le due trasposizioni hanno o non hanno una lettera comune. Essendo a, b, c, d quattro lettere diverse, si ha infatti

$$(a\,b)\;(a\,c) = (a\,b\,c)$$
$$(a\,b)\;(c\,d) = (b\,c\,d)\,.\;(a\,b\,c)\,.$$

E siccome ogni sostituzione pari si compone con prodotti contenenti ciascuno due trasposizioni, così qualunque sostituzione pari può comporsi con sostituzioni circolari su tre lettere, onde risulta evidente il teorema enunciato.

Il teorema superiore può facilmente generalizzarsi nella proposizione seguente:

Se un gruppo di sostituzioni sopra n lettere contiene tutte le sostituzioni circolari sopra r fra le n lettere ($r \geqq 2$), *esso coincide col gruppo totale.*

Per $r = 2$, essendovi nel gruppo tutte le trasposizioni, vi è certamente ogni altra sostituzione (§. 4). Per $r = 3$ il teorema è già stato sopra dimostrato. Infine il caso di $r > 3$ si riporta subito al precedente, osservando che ogni sostituzione ciclica di 3.° ordine si può comporre con due sostituzioni d'ordine $r > 3$, come si vede dall'identità

$$(x_1\,x_2\,x_3) = (x_1\,x_3\,x_2\,x_4\,\ldots\,x_r)\,.\,(x_1\,x_2\,x_3\,x_4\,\ldots\,x_r)^{-1}.$$

§. 9. — Rispetto ai gruppi di sostituzioni su lettere ha grande importanza la distinzione dei gruppi in due classi secondo i criterii seguenti.

Un gruppo G sopra n lettere

$$x_1\,x_2\,\ldots\,x_n$$

dicesi *transitivo* quando, prese due lettere ad arbitrio x_i, x_k fra le n, esiste sempre qualche sostituzione nel gruppo che porta x_i in x_k. In caso opposto il gruppo dicesi *intransitivo*. Per accertarsi della transitività di un gruppo basta esaminare se una lettera fissa, p. e. x_1, può essere portata, con sostituzioni del gruppo, in tutte le altre. E infatti se x_i, x_k sono due lettere arbitrarie, esisterà allora in G una sostituzione S che porterà x_1 in x_i ed una seconda S′ che porterà x_1 in x_k e la sostituzione $S^{-1}\,S'$ di G porterà x_i in x_k, onde il gruppo sarà transitivo.

Supponiamo che G sia un gruppo *intransitivo* e sia a_1 una qualunque delle n lettere. Indicheremo con

$$a_2,\;a_3,\ldots a_r$$

tutte le lettere in cui a_1 vien portata da sostituzioni del gruppo. Le r lettere

A] $$a_1 a_2 a_3 \ldots a_r$$

non esauriranno tutte le n lettere, sarà cioè $r < n$; altrimenti il gruppo sarebbe transitivo. Ora è chiaro, per quanto sopra si è visto, che le r lettere A] saranno congiunte fra loro transitivamente dal gruppo G, cioè si potrà portare, con una sostituzione di G, una qualunque di esse a_i in un'altra qualunque a_k; ma invece non esisterà alcuna sostituzione di G che porti una lettera del sistema A], p. e. a_i, fuori del sistema stesso, diciamo in b_1. E invero, nel caso opposto, una sostituzione di G porterebbe a_1 in b_1 contro l'ipotesi. Presa una lettera b_1 fra le n, fuori del sistema A], costruiremo medesimamente un sistema

B] $$b_1 b_2 \ldots b_s ,$$

sulle cui lettere il gruppo G agirà transitivamente, ma non porterà alcuna lettera del sistema B] fuori del sistema stesso. Così continuando, potremo scindere le n lettere, su cui opera il gruppo intransitivo, in un certo numero di sistemi

$$A] \ , \ B] \ , \ C] \ldots$$

così costituiti che le sostituzioni di G opereranno transitivamente entro ciascun sistema, ma non porteranno mai una lettera di un sistema in un'altra di sistema diverso. Diremo questi sistemi *sistemi di transitività*. Se il numero delle lettere nei rispettivi sistemi A], B], C]... è dato da

$$r, s, t \ldots ,$$

talchè $r + s + t + \ldots = n$, è facile vedere che:

L'ordine m del gruppo intransitivo G *sarà un divisore del prodotto* $\pi(r)\,\pi(s)\,\pi(t)\ldots$

Infatti ogni sostituzione di G consta di un fattore che opera solo sulle lettere di A], di un secondo che opera sulle lettere di B] ecc. Se costruiamo i gruppi totali

$$\Gamma_{\pi(r)}, \ \Gamma_{\pi(s)}, \ \Gamma_{\pi(t)}$$

sulle lettere dei rispettivi sistemi A], B], C]... e facciamo il prodotto di tutti questi gruppi parziali, costruendo cioè tutti i possibili prodotti

di una sostituzione di $\Gamma_{\pi(r)}$, per una di $\Gamma_{\pi(s)}$, per una di $\Gamma_{\pi(t)}$ ecc., avremo un gruppo d'ordine $\pi(r)\ \pi(s)\ \pi(t)\ldots$, che conterrà G come sottogruppo.

Ritorniamo ai gruppi transitivi per distinguerli a seconda del *grado di transitività. Un gruppo* G *sopra* n *lettere dicesi* m *volte transitivo quando, scelti due sistemi arbitrarii di* m *lettere ciascuno fra le* n, *e fissato ad arbitrio l'ordine delle* m *lettere in ciascuno, esiste sempre nel gruppo qualche sostituzione che porta le prime* m *lettere ordinatamente nelle seconde.*

Come per la semplice transitività, si vedrà anche qui che il gruppo è m volte transitivo se possono portarsi con sostituzioni del gruppo m lettere fisse in m arbitrarie. Naturalmente se un gruppo è m volte transitivo, lo è a più forte ragione $m-1$, $m-2\ldots$ volte; ma generalmente, quando parliamo di un gruppo m volte transitivo, intendiamo che non lo sia $m+1$ volte.

Esempî di gruppi a transitività multipla li abbiamo nel gruppo alterno $G_{\frac{\pi(n)}{2}}$ e nel gruppo totale $G_{\pi(n)}$. Il primo è precisamente $n-2$ volte transitivo, poichè se

$$x_{i_1}\, x_{i_2}\ldots x_{i_{n-1}}\, x_{i_n}$$

è una permutazione qualsiasi delle n lettere, fra le due sostituzioni:

$$\begin{pmatrix} x_{i_1}\, x_{i_2}\ldots x_{i_{n-1}}\, x_{i_n} \\ x_1\ x_2\ \ldots x_{n-1}\ x_n \end{pmatrix}, \quad \begin{pmatrix} x_{i_1}\, x_{i_2}\ldots x_{i_n}\ \ x_{i_{n-1}} \\ x_1\ x_2\ \ldots x_{n-1}\, x_n \end{pmatrix},$$

che differiscono per una trasposizione, una appartiene al gruppo alterno.

Quanto al gruppo totale, potrebbe riguardarsi, stando alla definizione, come n volte transitivo; ma siccome, fissate $n-1$ lettere, ne resta una perfettamente determinata, converrà riguardarlo come $n-1$ volte transitivo. È evidente del resto che un gruppo $n-1$ volte transitivo su n lettere coincide col gruppo totale.

§. 10. — Dimostriamo il seguente teorema fondamentale sui gruppi transitivi.

L'ordine N *di un gruppo* G, m *volte transitivo su* n *lettere, è dato da*

$$N = k\,.\,n\ (n-1)\ldots(n-m+1),$$

dove k *è l'ordine di quel sottogruppo di* G *che lascia ferme* m *lettere fissate ad arbitrio.*

Prendiamo, ad esempio, le prime m lettere

$$x_1 x_2 \ldots x_m$$

e sia

$$\Gamma = (\gamma_1 \gamma_2 \gamma_3 \ldots \gamma_k)$$

quel sottogruppo di G che lascia ferma *ciascuna* di queste lettere. Distribuiamo le sostituzioni di G rispetto al sottogruppo Γ nel solito quadro:

$$G = \left\{ \begin{array}{l} \gamma_1, \gamma_2, \ldots \gamma_k \\ \gamma_1 t_2, \gamma_2 t_2 \ldots \gamma_k t_2 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \gamma_1 t_q, \gamma_2 t_q, \ldots \gamma_k t_q, \end{array} \right.$$

avendo indicato con q l'indice di Γ in G.

Due sostituzioni di G portano le lettere

$$x_1 x_2 \ldots x_m$$

nel medesimo sistema di posti, o in sistemi diversi, secondo che esse trovansi nel quadro in una medesima orizzontale o in orizzontali diverse. La prima cosa è evidente e quanto alla seconda si osservi che, se g, g' hanno sopra $x_1, x_2 \ldots x_m$ il medesimo effetto, la $g' g^{-1}$ lascia ferme queste m lettere ed è per ciò una γ onde

$$g' = \gamma_i g$$

e g, g' trovansi nella medesima orizzontale del quadro. Ciò posto, siccome G è m volte transitivo, il numero q dei sistemi di posti diversi, in cui le m lettere possono portarsi, eguaglia il numero delle disposizioni delle n lettere m ad m, cioè si ha appunto

$$q = n(n-1) \ldots (n-m+1) \qquad \text{c. d. d.}$$

Dimostriamo ora l'altro teorema:

In un gruppo G *m volte transitivo, che non coincida col gruppo alterno o col gruppo totale, non può esistere alcuna sostituzione (eccetto l'identità) che sposti m lettere soltanto o meno di m lettere.*

Siccome ogni sostituzione non identica sposta due lettere almeno, supponiamo naturalmente $m \geq 2$. Ora sia S, se è possibile, una sostituzione di G che operi sopra m lettere al massimo e indichiamo con

T una sostituzione di G che porti queste m lettere in altre m arbitrarie, come ne esiste certamente a causa della transitività multipla. Anche la $T^{-1} S T$, che è una qualunque sostituzione simile ad S, trovasi in G. Se decomponiamo S in cicli, dovremo avere almeno due cicli effettivi; altrimenti G, contenendo tutte le sostituzioni simili ad S, cioè tutte le sostituzioni circolari di un dato ordine, sarebbe il gruppo alterno o totale (§. 8). Fra i cicli di S ve ne sia dapprima almeno uno d'ordine ≥ 3 e sia

$$C_1 = (x_1 x_2 x_3 \ldots x_r).$$

Prendiamo una sostituzione S′ simile ad S che contenga il ciclo

$$(x_1 x_3 x_2 \ldots x_r)$$

e gli altri cicli di S. Anche la S′ sarà in G, per quanto si è visto, quindi anche

$$S' S^{-1} = (x_1 x_2 x_3)$$

che è ciclica del 3.° ordine, onde G sarebbe il gruppo alterno o totale.

Supponiamo in fine che tutti i cicli di S siano del 2.° ordine e quindi in numero di due almeno, per cui certamente $m \geq 4$; sia

$$S = (a_1 a_2)(a_3 a_4)(a_5 a_6) \ldots$$

Prendasi la sostituzione simile

$$S' = (a_1 a_3)(a_2 a_4)(a_5 a_6) \ldots$$

e si avrà in G anche

$$U = S S' = (a_1 a_4)(a_2 a_3).$$

Ma, essendo $m \geq 4$, quindi $n \geq 5$, vi sarà almeno una 5.ª lettera a_5 e in G la sostituzione U′ simile ad U

$$U' = (a_1 a_5)(a_2 a_3),$$

onde anche la $U U' = (a_1 a_4 a_5)$, ciò che ci riconduce al caso precedente.

§. 11. — I teoremi sui gruppi transitivi, dimostrati al §. precedente, insieme alle nuove proposizioni, che ora stabiliremo, servono a fissare un limite superiore pel grado di transitività di un gruppo. Premettiamo il lemma seguente:

Se un gruppo G *d'ordine* m *contiene due sottogruppi* Γ, Γ' *dei rispettivi ordini* n, n' *e non esiste in* Γ' *(l'identità esclusa) alcuna sostituzione simile ad una sostituzione di* Γ, *sarà l'ordine* m *del gruppo multiplo del prodotto* $n \cdot n'$ *degli ordini dei sottogruppi.*

Siano

$$\Gamma = (\gamma_1 , \gamma_2 , \gamma_3 , \ldots \gamma_n)$$

$$\Gamma' = (\gamma'_1, \gamma'_2, \gamma'_3, \ldots \gamma'_{n'})$$

i due sottogruppi e formiamo le $n\,n'$ sostituzioni di G

$$\alpha) \qquad \gamma_i \, \gamma'_k \begin{cases} i = 1, 2, 3 \ldots n \\ k = 1, 2, 3 \ldots n' \end{cases}$$

Queste sono tutte distinte fra loro perchè, se fosse

$$\gamma_i \gamma'_k = \gamma_j \gamma'_\lambda ,$$

avremmo

$$\gamma_j^{-1} \gamma_i = \gamma'_\lambda \, \gamma'^{-1}_k ,$$

cioè una sostituzione di Γ eguaglierebbe una di Γ', ciò che ha luogo soltanto, per ipotesi, per la sostituzione identica, onde risulterebbe

$$\gamma_i = \gamma_j \ , \ \gamma'_k = \gamma'_\lambda \ .$$

Se le α) esauriscono tutte le sostituzioni di G si ha $m = n\,n'$ ed il teorema è verificato. In caso opposto, sia g una sostituzione di G, oltre le $n\,n'$ in α), e si costruisca la nuova serie

$$\beta) \qquad \gamma_i \, g \, \gamma'_k \begin{cases} i = 1, \ 2, \ 3 \ldots n \\ k = 1, \ 2, \ 3 \ldots n'. \end{cases}$$

Queste $n\,n'$ sostituzioni di G sono diverse fra loro e dalle α). E infatti da

$$\gamma_i \, g \, \gamma'_k = \gamma_j \, g \, \gamma'_\lambda \ ,$$

seguirebbe

$$g^{-1} (\gamma_j^{-1} \gamma_i) \, g = \gamma'_\lambda \, \gamma'^{-1}_k$$

e però le due sostituzioni

$$\gamma_j^{-1} \gamma_i \ , \ \gamma'_\lambda \, \gamma'^{-1}_k$$

l'una di Γ, l'altra di Γ', sarebbero simili fra loro. Dunque ambedue sono l'identità e si ha quindi

$$\gamma_i = \gamma_j \ , \ \gamma'_k = \gamma'_\lambda \ .$$

Se poi una β) eguagliasse una α), p. e. si avesse

$$\gamma_i \, g \, \gamma'_k = \gamma_j \, \gamma'_\lambda$$

ne dedurremmo

$$g = (\gamma_i^{-1} \gamma_j) \cdot (\gamma'_\lambda \, \gamma'^{-1}_k)$$

e la g sarebbe in α) contro l'ipotesi.

Così procedendo come nella dimostrazione del teorema fondamentale (§. 7), vediamo che le sostituzioni di G si distribuiscono in un certo numero di orizzontali contenenti $n\,n'$ sostituzioni ciascuna, ciò che dimostra il teorema.

Ciò premesso, possiamo ora dimostrare la proposizione seguente:

L'ordine N *di un gruppo* G *m volte transitivo su n lettere, che non coincida col gruppo alterno o totale, è un divisore del numero*

$$\frac{\pi(n)}{\pi(m)} = (m+1)(m+2)\ldots n$$

Per dimostrarla, formiamo il gruppo totale $\Gamma_{\pi(m)}$ sopra m lettere fissate ad arbitrio fra le n. I due gruppi G e $\Gamma_{\pi(m)}$, in ciascuno dei quali non esiste, pel teorema alla fine del §. 10, alcuna sostituzione simile ad una dell'altro, sono ambedue contenuti nel gruppo totale d'ordine $\pi(n)$ sulle n lettere; dal lemma superiore segue quindi che $\pi(n)$ è divisibile pel prodotto N $\pi(m)$, cioè N divide $\frac{\pi(n)}{\pi(m)}$ c. d. d.

D'altronde, se ricordiamo (§. 10) che N deve essere multiplo di

$$n\,(n-1)\ldots\ldots(n-m+1)\,,$$

vediamo che

$$n\,(n-1)\ldots(m+1)$$

deve essere divisibile per

$$n\,(n-1)\ldots(n-m+1)$$

e perciò

$$n-m \geq m\,,$$

ossia $m \leq \frac{n}{2}$. Indicando con $\left[\frac{n}{2}\right]$ il massimo intero contenuto in $\frac{n}{2}$, possiamo quindi enunciare il risultato seguente:

Un gruppo di sostituzioni sopra n lettere, che non coincida col gruppo alterno o col gruppo totale, non può essere più di $\left[\frac{n}{2}\right]$ *volte transitivo.*

A questo limite superiore $\left[\frac{n}{2}\right]$ del grado di transitività di un gruppo se ne potrebbero sostituire altri molto più piccoli coll'uso di ulteriori teoremi. Ma noi ci limiteremo al risultato conseguito, che serve già a rilevare come il gruppo alterno e totale si distinguano, pel loro grado più alto di transitività, da tutti gli altri gruppi.

§. 12. — Per i gruppi di sostituzioni sopra lettere è importante anche la classificazione in gruppi *imprimitivi* e *primitivi*, di cui ci andiamo ora ad occupare.

Un gruppo transitivo G dicesi *imprimitivo* quando le n lettere, su cui opera il gruppo, possono scindersi in sistemi, contenenti ciascuno un egual numero di lettere, per modo che le sostituzioni di G o lascino ciascuna lettera di un sistema nel proprio sistema, o portino contemporaneamente tutte le lettere di un sistema in tutte quelle di un altro sistema. Se è impossibile scindere le lettere in tali sistemi, il gruppo dicesi *primitivo*. Così p. e., rispetto al gruppo transitivo ciclico su 6 lettere formato dalle potenze della sostituzione circolare

$$S = (x_1\, x_2\, x_3\, x_4\, x_5\, x_6),$$

i due sistemi di tre lettere ciascuno

$$x_1\, x_3\, x_5 \;,\; x_2\, x_4\, x_6,$$

sono appunto sistemi d'imprimitività.

Notiamo subito che un gruppo può essere in più modi imprimitivo, cioè può darsi che la divisione in sistemi d'imprimitività possa farsi in diverse maniere. Così, nel caso sopra citato, anche i tre sistemi di due lettere

$$x_1\, x_4 \;,\; x_2\, x_5 \;,\; x_3\, x_6$$

formano sistemi d'imprimitività.

Un gruppo dotato di transitività multipla non può mai essere imprimitivo, poichè potendosi portare, con sostituzioni del gruppo, due lettere arbitrarie in altre due arbitrarie, la divisione in sistemi d'imprimitività è impossibile. Dunque: *ogni gruppo più volte transitivo è primitivo.*

Così pure è chiaro che: *ogni gruppo transitivo sopra un numero primo di lettere è necessariamente primitivo.*

Sia G un gruppo imprimitivo. Quelle sostituzioni di G che lasciano fisso ciascun sistema d'imprimitività formano evidentemente in G un sottogruppo Γ, che può del resto anche ridursi alla identità. Se distribuiamo le sostituzioni di G rispetto a quelle di Γ nel solito quadro

$$G = \left\{ \begin{array}{l} \Gamma \\ \Gamma t_2 \\ \Gamma t_3 \\ \vdots \\ \Gamma t_q \,, \end{array} \right.$$

vediamo subito che due sostituzioni di G producono sui sistemi d'imprimitività la medesima permutazione allora ed allora soltanto che appartengono ad una medesima orizzontale. Considerando quindi questi sistemi come altrettanti elementi (lettere)

$$A\,,\ B\,,\ C \ldots,$$

il gruppo G produrrà su di essi un gruppo di sostituzioni H, d'ordine eguale all'indice q di Γ in G. Se r è il numero dei sistemi, sarà quindi q un divisore $\pi(r)$.

§. 13. — Vi è un caso importante in cui dalla specie delle sostituzioni del gruppo si può concludere la sua imprimitività, come insegna il teorema seguente:

Se un gruppo transitivo contiene una trasposizione, esso è imprimitivo, ovvero coincide col gruppo totale.

Il gruppo transitivo G sulle n lettere

$$x_1\,,\ x_2\,,\ x_3 \ldots x_n$$

contenga la trasposizione $(x_1 x_2)$. Se esso contenesse anche tutte le trasposizioni

$$(x_1 x_3) \ , \ (x_1 x_4) \ldots (x_1 x_n) \ ,$$

conterrebbe qualsiasi trasposizione $(x_i x_k)$, come si vede dalla identità

$$(x_i x_k) = (x_1 x_i) \ (x_1 x_k) \ (x_1 x_i) \ ,$$

e per ciò coinciderebbe col gruppo totale. Siano dunque

$$(x_1 x_2) \ , \ (x_1 x_3) \ldots (x_1 x_r) \quad (r < n)$$

tutte le trasposizioni di G contenenti x_1.

Per l'osservazione ora fatta, il gruppo G conterrà il gruppo totale sulle r lettere

A] $$x_1 \ x_2 \ x_3 \ldots x_r \ ;$$

ma non vi sarà in G alcun'altra trasposizione, che congiunga una lettera del sistema A] con una fuori di esso. E invero, se in G avessimo p. e. la trasposizione

$$(x_i \ x_{r+1}) \ ,$$

avremmo anche la trasposizione

$$(x_1 x_{r+1}) = (x_1 x_i) \ (x_i x_{r+1}) \ (x_1 x_i)$$

contro l'ipotesi. Poichè il gruppo G è transitivo, presa una lettera qualunque x_{i_1} fuori di A], avremo in G una sostituzione T che porta x_1 in x_{i_1}; supponiamo che sulle r lettere A] la T abbia l'effetto

$$\mathrm{T} = \begin{pmatrix} x_{i_1} \ x_{i_2} \ldots x_{i_r} \ldots \\ x_1 \ x_2 \ldots x_r \ldots \end{pmatrix}$$

e consideriamo il sistema

B] $$x_{i_1} \ x_{i_2} \ldots x_{i_r}$$

Avremo in G le trasposizioni

$$\mathrm{T}^{-1} (x_1 x_2) \ \mathrm{T} \ , \ \mathrm{T}^{-1} (x_1 x_3) \ \mathrm{T} \ldots \mathrm{T}^{-1} (x_1 x_r) \ \mathrm{T} \ ,$$

cioè

$$(x_{i_1} x_{i_2}) \ , \ (x_{i_1} x_{i_3}) \ldots (x_{i_1} x_{i_r}) \ ,$$

onde anche le r lettere del sistema B] saranno tutte congiunte due a due per trasposizioni di G; segue, per quanto si è visto sopra, che,

essendo x_{i_1} fuori di A], anche tutte le altre lettere di B] sono fuori di A]. D'altronde nessun'altra lettera fuori di B] potrà essere congiunta per trasposizioni di G con x_{i_1}, altrimenti la sostituzione inversa di T la porterebbe in una lettera fuori di A] e congiunta per trasposizioni di G con x_1. Il nuovo sistema B] è formato quindi precisamente come il sistema A] e contiene un egual numero di lettere. Così proseguendo, è chiaro che distribuiremo le n lettere in un certo numero s di sistemi contenenti un egual numero di lettere

$$A\ ,\ B\ ,\ C \ldots ,$$

ciascun sistema contenendo tutte e sole quelle lettere che sono congiunte, per trasposizioni di G, ad una (qualsiasi) di esse. Applicando alle lettere di uno di questi sistemi una sostituzione qualunque di G, le nuove lettere costituiscono un sistema della medesima specie. Dunque il gruppo G opera imprimitivamente sui sistemi A, B, C..., il che dimostra il teorema.

Dal teorema così dimostrato risulta il corollario:

Se un gruppo transitivo sopra un numero primo di lettere contiene una trasposizione, coincide col gruppo totale.

Capitolo II.

Isomorfismo dei gruppi. — Composizione dei gruppi. — Teorema di Jordan. — Serie principale di composizione. — Teorema di Hölder. — I due teoremi di Sylow. — Gruppi semplici degli ordini da 1 a 100.

§. 14. — Le proprietà dei gruppi, delle quali ci andiamo ad occupare nel presente capitolo, hanno una grande importanza come quelle che si riferiscono alla teoria generale dei gruppi di operazioni.

Stabiliamo in primo luogo il concetto d'*isomorfismo* dei gruppi. Siano G, Γ due gruppi di sostituzioni (operazioni) del medesimo ordine m:

$$G = (g_1\ ,\ g_2\ ,\ g_3 \cdots g_m)$$
$$\Gamma = (\gamma_1\ ,\ \gamma_2\ ,\ \gamma_3 \cdots \gamma_m)$$

e supponiamo che si possa stabilire fra le sostituzioni dei due gruppi una corrispondenza biunivoca, tale cioè che ad ogni sostituzione di G ne corrisponda una perfettamente determinata in Γ ed inversamente,

colla condizione essenziale che: *al prodotto di due qualunque sostituzioni di* G *corrisponda in* Γ *il prodotto delle due sostituzioni corrispondenti.*

I due gruppi si diranno allora *isomorfi*, ovvero in corrispondenza di *isomorfismo.*

Per fissare le idee, supponiamo che ad una sostituzione g_i di G corrisponda la γ_i col medesimo indice in Γ. È facile vedere che: *All'identità in* G *deve corrispondere l'identità in* Γ. Infatti se γ corrisponde a 1 in G, al prodotto $1 . g_i = g_i$ corrisponde in Γ il prodotto $\gamma . \gamma_i$, che è dunque $= \gamma_i$, onde $\gamma = 1$. Per la legge fondamentale d'isomorfismo, al prodotto $g_i g_k$, corrisponderà il prodotto $\gamma_i \gamma_k$, in particolare alle potenze

$$g_i^2 , g_i^3 , g_i^4 \ldots$$

di g_i corrisponderanno le potenze di eguale esponente di γ_i

$$\gamma_i^2 , \gamma_i^3 , \gamma_i^4 \ldots .$$

onde risulta: *Due sostituzioni corrispondenti* g_i, γ_i *hanno sempre egual periodo.* E infatti se β è il periodo di g_i e β' quello di γ_i, siccome

$$g_i^\beta = 1 ,$$

sarà anche

$$\gamma_i^\beta = 1 ,$$

onde β è multiplo di β'; per la medesima ragione β' è multiplo di β, quindi $\beta = \beta'$.

È immediatamente evidente il teorema:

Ad ogni sottogruppo G_1 *di* G *corrisponde in* Γ *un sottogruppo* Γ_1 *di ordine eguale a* G_1.

La nozione d'isomorfismo fra i gruppi si può estendere anche al caso di gruppi che non siano del medesimo ordine.

Essendo ancora G, Γ due gruppi, ma non più del medesimo ordine, supponiamo che ad una sostituzione di G ne corrisponda sempre una sola in Γ, ma la corrispondenza non sia più biunivoca che cioè ad una medesima sostituzione in Γ ne corrispondano diverse in G, supponendo per altro sempre soddisfatta la legge fondamentale che *al prodotto di due g corrisponda in* Γ *il prodotto delle corrispondenti.* Diremo allora che il gruppo G è in corrispondenza d'isomorfismo *meriedrico* con Γ, mentre nel caso speciale sopra considerato che G, Γ abbiano il medesimo ordine l'isomorfismo si dirà *holoedrico.*

Anche se l'isomorfismo è meriedrico si concluderà, come sopra, che all'identità in G corrisponde l'identità in Γ. Ma riguardo ai periodi di due sostituzioni corrispondenti g, γ si potrà soltanto concludere che *il periodo di γ è un divisore del periodo di g*. In ogni caso però a $g^{-1} = g^{\beta} \,.\, g^{-1}$ corrisponderà $\gamma^{\beta} \,.\, \gamma^{-1} = \gamma^{-1}$.

Come esempii d'isomorfismo oloedrico o meriedrico, citiamo i seguenti. Consideriamo attorno ad un asse fisso nello spazio tutte le rotazioni di ampiezza eguale a un multiplo di $\frac{2\pi}{n}$ (n intero qualunque); esse formano un gruppo di rotazioni d'ordine n, che è oloedricamente isomorfo col gruppo ciclico generato dalle potenze della sostituzione ciclica d'ordine n

$$S = (x_1 x_2 x_3 \ldots x_n).$$

In secondo luogo sia S una sostituzione (operazione) di periodo composto $m = p\,q$ ed U una sostituzione a periodo p. I due gruppi ciclici

$$G = (1, S, S^2, \ldots S^{m-1})$$
$$\Gamma = (1, U, U^2, \ldots U^{p-1})$$

saranno posti in corrispondenza d'isomorfismo meriedrico, facendo corrispondere ad ogni potenza S^n di S quella potenza U^r di U che ha per esponente il minimo resto positivo di n (mod p).

Riprendendo le considerazioni generali, supponiamo che G sia in corrispondenza d'isomorfismo meriedrico con Γ e all'identità in Γ corrispondano G le n sostituzioni

$$\sigma_1 = 1, \sigma_2, \sigma_3 \ldots \sigma_n,$$

fra le quali deve naturalmente trovarsi l'identità. Queste sostituzioni σ formano un sottogruppo Σ di G, poichè al prodotto $\sigma_i\,\sigma_k$ in G corrisponde in Γ il prodotto $1 \,.\, 1 = 1$. Distribuiamo ora le sostituzioni di G rispetto al sottogruppo Σ nel quadro

$$G = \left\{ \begin{array}{l} \Sigma \\ \Sigma t_2 \\ \vdots \\ \Sigma t_q, \end{array} \right.$$

essendo q l'indice di Σ in G. Si vede subito che a due sostituzioni

identiche o diverse g, g' di G corrispondono in Γ sostituzioni identiche o diverse, secondo che g, g' appartengono alla medesima o a diverse orizzontali del quadro [1]). Abbiamo dunque il risultato: *Se il gruppo* G *è in isomorfismo meriedrico con* Γ *e alla identità in* Γ *corrispondono le* n *sostituzioni*

$$\sigma_1 \, \sigma_2 \ldots \sigma_n$$

in G, *queste formano un sottogruppo di* G *e ad ogni altra sostituzione in* Γ *ne corrisponderanno* n *diverse in* G.

Questo numero n dicesi il *grado di meriedria*. È chiaro che ad ogni sottogruppo Γ_1 di Γ corrisponde in G un sottogruppo G_1, il cui ordine è n volte quello di Γ_1; e perciò G_1 ha il medesimo indice in G come Γ_1 in Γ.

§. 15. — Stabilito il concetto d'isomorfismo dei gruppi, possiamo vedere come lo studio dei gruppi generali *finiti* di operazioni, quando sono soddisfatte le leggi fondamentali già ricordate al §. 6, si riconduca a quello dei gruppi di sostituzioni sopra lettere.

Supponiamo di considerare una serie di operazioni, di qualunque natura esse siano, ma per le quali valgano le leggi fondamentali seguenti:

1.° Esista una legge di composizione per la quale da due operazioni A, B della serie se ne deduca una terza determinata, eseguendo prima A poi B; questa terza operazione (prodotto delle due) si indichi con AB.

2.° Senza valere in generale la legge permutativa dei fattori, valga però la legge associativa, espressa, nel caso elementare, da

$$(AB)\,C = A\,(BC).$$

3.° Dall'identità $AB = AC$, o dall'altra $BA = CA$, segua necessariamente $B = C$.

Supponiamo ora di avere un gruppo finito G di tali operazioni

$$a) \qquad A_1, \; A_2, \ldots A_m .$$

Se le moltiplichiamo tutte da una medesima parte, p. e. a destra, per una fissa di esse, sia A_i, le m operazioni

$$b) \qquad A_1 A_i, \; A_2 A_i, \ldots A_m A_i$$

---

[1]) Se g, g' corrispondono alla medesima γ, al prodotto $g' \, g^{-1}$ corrisponde $\gamma' \gamma^{-1} = 1$ e però $g' g^{-1} = \sigma_i$, $g' = \sigma_i \, g$.

sono tutte fra le $A_1 A_2 \ldots A_m$, che per ipotesi formano gruppo; inoltre, per la 3.ª proprietà supposta, non vi sono in *b*) due operazioni identiche, onde le *b*) riproducono in altro ordine le *a*). Riguardando A_1, $A_2 \ldots A_m$ come altrettanti oggetti (lettere), si passa dalla permutazione *a*) alla *b*) con una sostituzione S_i sulle m lettere A_i; si avrà precisamente

$$S_i = \begin{pmatrix} A_1 A_i, & A_2 A_i \ldots A_m A_i \\ A_1 \;, & A_2 \;\ldots\; A_m \end{pmatrix}.$$

Si vede subito che, se S_i, S_k sono le sostituzioni corrispondenti alle operazioni A_i, A_k, e si ha $A_i A_k = A_j$, sarà anche $S_i S_k = S_j$. Le m sostituzioni

$$S_1, S_2, \ldots S_m,$$

che sono tutte fra loro distinte, a causa della 3.ª proprietà, formano un gruppo Γ di m sostituzioni sulle m lettere

$$A_1 \; A_2 \ldots A_m,$$

che è in isomorfismo oloedrico con G ed è semplicemente transitivo. Dunque:

A qualunque gruppo finito G *di m operazioni si può porre in corrispondenza d'isomorfismo oloedrico un gruppo* Γ *semplicemente transitivo di m sostituzioni sopra m lettere.*

Siccome in Γ vi è certamente la identità, così anche in G vi è certamente un'operazione A_1, da indicarsi come *unità*, che composta con qualunque altra operazione di G dà l'operazione stessa. Così pure, date due operazioni qualunque

$$A_i, \; A_k,$$

ve ne è sempre una terza determinata A_j, per la quale

$$A_i A_j = A_k.$$

In particolare se $A_k = A_1$ è l'operazione unitaria A_1, la A_j si dirà l'inversa di A_i e si indicherà con A_i^{-1} ecc.

Se consideriamo due gruppi di operazioni G, G′ del medesimo ordine ed oloedricamente isomorfi e, prescindendo dal significato speciale delle operazioni nei singoli gruppi, abbiamo soltanto riguardo al modo come si compongono fra loro le operazioni in G e in G′, è chiaro che i due gruppi sono da riguardarsi come astrattamente identici. Così adunque

dal punto di vista astratto, ad ogni gruppo finito di operazioni possiamo sostituire un gruppo di sostituzioni sopra lettere.

§. 16. — Sia G un gruppo di sostituzioni d'ordine m:

$$G = (g_1, g_2, \ldots g_m)$$

e T una sostituzione qualunque sulle medesime lettere. Le m sostituzioni trasformate delle g per mezzo della T

$$T^{-1} g_1 T, \; T^{-1} g_2 T, \ldots T^{-1} g_m T$$

formano evidentemente (§. 5) un nuovo gruppo G_1; questo dicesi il gruppo trasformato di G per mezzo di T e si scrive

$$G_1 = T^{-1} G T.$$

I due gruppi G, G_1, cangiata denominazione alle lettere, sono in sostanza identici. Può accadere che il gruppo G_1 coincida assolutamente con G, cioè

$$T^{-1} G T = G;$$

allora si dice che la *sostituzione* T *è permutabile col gruppo* G. Ciò avviene in particolare se T appartiene a G ed anche se T è permutabile colle *singole* sostituzioni di G. Quando T sia permutabile con G, presa una qualunque sostituzione g_i di G, avremo

$$T^{-1} g_i T = g_k,$$

cioè

$$g_i T = T g_k.$$

Sia G un gruppo e Γ un suo sottogruppo. Trasformando Γ con una qualunque sostituzione di G, il gruppo trasformato

$$\Gamma_1 = g^{-1} \Gamma g$$

è ancora un sottogruppo di G, che in particolare coinciderà con Γ stesso, se g è permutabile con Γ. *Quando avvenga che il sottogruppo* Γ *sia permutabile con tutte le sostituzioni del gruppo* G, *si dice che il sottogruppo* Γ *è invariante od eccezionale in* G.

Noi adotteremo la prima denominazione che viene usata, in senso perfettamente analogo, da Lie nella teoria dei gruppi continui di trasformazioni.

Come esempio di sottogruppo invariante citiamo il gruppo alterno nel gruppo totale. Così pure, in un gruppo G di sostituzioni a due a due permutabili, qualunque sottogruppo è invariante.

Un altro esempio molto importante è il seguente. Sia G un gruppo in isomorfismo meriedrico con un gruppo Γ, all'identità in Γ corrispondendo il sottogruppo

$$\sum = (\sigma_1 \sigma_2 , \ldots \sigma_n)$$

in G. *Il sottogruppo* Σ *sarà invariante in* G. E infatti, se g è una qualunque sostituzione in G, a $g^{-1} \sigma_i g$ corrisponde in Γ la $\gamma^{-1} . 1 . \gamma = 1$.

Un sottogruppo Γ invariante di un gruppo G dicesi *invariante massimo* quando non esiste in G alcun altro sottogruppo invariante Λ contenente Γ e più ampio di questo. Si osservi che un sottogruppo Γ invariante in G sarà certamente invariante massimo se l'indice di Γ in G è un numero primo, come accade p. e. pel gruppo alterno nel gruppo totale.

In ogni gruppo G esistono, nel senso stretto, almeno due sottogruppi invarianti, cioè G stesso e l'identità. Un gruppo G che non possieda alcun altro sottogruppo invariante dicesi un *gruppo semplice;* in caso contrario, quando cioè G ammetta un sottogruppo puro invariante d'ordine > 1, il gruppo si dirà composto.

Da quanto sopra si è visto risulta che un gruppo semplice G non può esser posto con un altro gruppo Γ in altra relazione d'isomorfismo che oloedrico.

§. 17. — Le nozioni stabilite nel §. precedente sono d'importanza fondamentale per lo studio della *composizione* dei gruppi. Ma, prima di esporre le teorie che ne derivano, conviene che ci tratteniamo alquanto sulla formazione del così detto *gruppo complementare* di un gruppo G rispetto ad un suo sottogruppo Γ.

Sia G un gruppo d'ordine m e Γ un suo sottogruppo d'ordine n, che supponiamo dapprima qualunque (invariante o no), e sia q l'indice di Γ in G. Diciamo equivalenti (a sinistra) due sostituzioni g, g' rispetto a Γ e scriviamo

$$g' \equiv g ,$$

quando sussista un'eguaglianza della forma

$$g' = \gamma g .$$

essendo γ una sostituzione del sottogruppo Γ. Siccome ne segue $g = \gamma^{-1} g'$, vediamo che questa nozione di equivalenza è invertibile. Inoltre due sostituzioni g', g'', equivalenti ad una terza g, sono equivalenti fra loro. In simboli da

$$g' = \gamma g \ , \ g'' = \gamma' g$$

segue

$$g'' = \gamma' \gamma^{-1} \cdot g',$$

cioè $g'' \equiv g'$. Potremo quindi ripartire le sostituzioni di G in classi di sostituzioni equivalenti rispetto a Γ, ponendo in una medesima classe tutte e sole quelle che sono equivalenti ad una medesima, quindi fra loro. Se ripartiamo le sostituzioni di G nel solito quadro rispetto a Γ

$$G = \left\{ \begin{array}{l} \Gamma \\ \Gamma g_2 \\ \Gamma g_3 \\ \vdots \\ \Gamma g_q, \end{array} \right.$$

si vede subito che due sostituzioni di G appartengono o no alla medesima classe, secondo che figurano nel quadro nella medesima orizzontale od in orizzontali diverse. Estraendo da ogni classe, ad arbitrio, una sostituzione, formeremo un sistema

$$a) \qquad g_1, g_2, g_3 \cdots, g_q,$$

che si potrà dire un *sistema completo* di rappresentanti delle classi, in quanto che ogni sostituzione di G sarà equivalente ad una e ad una sola fra queste.

Ora moltiplichiamo *a destra* tutte le q sostituzioni a) per una medesima g di G. Ciascuna delle q sostituzioni

$$b) \qquad g_1 g, \ g_2 g, \ g_3 g, \ \ldots g_q g$$

troverà la propria equivalente in una ed una sola delle a). E poichè non può essere

$$g_i g \equiv g_k g$$

per $i \neq k$, altrimenti ne seguirebbe evidentemente $g_i \equiv g_k$, le b) saranno equivalenti, in altro ordine, alle a), diciamo p. e. rispettivamente a

$$b^*) \qquad g_{i_1} g_{i_2} \cdots g_{i_q},$$

essendo $i_1 i_2 \ldots i_q$ una permutazione degli indici 1, 2, ... q. Dalla permutazione a) delle q lettere $g_1 g_2 \ldots g_q$ si passa alla permutazione b*) mediante una sostituzione h, che diciamo corrispondente alla moltiplicatrice g. Ora, se alle due sostituzioni moltiplicatrici g, g' corrispondono sui simboli a) le sostituzioni h, h', è evidente che al prodotto $g\,g'$ corrisponderà il prodotto $h\,h'$. Quindi; *L'insieme delle sostituzioni h sulle q classi (od orizzontali del quadro) costituisce un gruppo* H, *col quale il gruppo dato* G *è isomorfo, ad ogni sostituzione in* G *corrispondendone una sola in* H.

Questo gruppo H si dirà il *gruppo complementare* (a destra) del gruppo G, rispetto al sottogruppo Γ, e si scriverà col simbolo di quoziente

$$\mathrm{H} = \frac{\mathrm{G}}{\Gamma}\,.$$

È naturale ora la domanda: *L'isomorfismo del gruppo* G *col gruppo complementare* $\mathrm{H} = \frac{\mathrm{G}}{\Gamma}$ *è oloedrico o meriedrico?*

Per decidere la questione, bisogna ricercare se vi è qualche sostituzione g di G, non identica, cui corrisponda l'identica in H. Si dovrà avere in tal caso, per tutti i valori di i da 1 a q

$$g_i\, g \equiv g_i\,,$$

cioè

$$g = g_i^{-1}\, \gamma\, g_i\,,$$

essendo γ una sostituzione di Γ. Ora, trasformando Γ con *tutte* le sostituzioni di G, si ottengono al massimo i q sottogruppi trasformati

$$\Gamma,\ g_2^{-1}\,\Gamma\, g_2,\ g_3^{-1}\,\Gamma\, g_3, \ldots g_q^{-1}\,\Gamma\, g_q\,,$$

che possono del resto tutti od in parte coincidere. La considerazione superiore dimostra che alla sostituzione g corrisponderà nel gruppo complementare allora ed allora soltanto l'identità, quando g appartenga a *tutti* i sottogruppi trasformati di Γ, cioè al loro sottogruppo Σ comune.

La risposta alla domanda superiore è adunque la seguente: *All'identità nel gruppo complementare* $\mathrm{H} = \frac{\mathrm{G}}{\Gamma}$ *corrispondono in* G *tutte e sole le sostituzioni del sottogruppo* Σ *comune a* Γ *e a tutti i suoi sottogruppi trasformati in* G. L'isomorfismo sarà dunque meriedrico od oloedrico, secondo che Σ non si ridurrà o si ridurrà all'identità.

Quest'ultimo caso avviene necessariamente, se G è un gruppo semplice.

Si osservi il caso particolare più importante in cui Γ è sottogruppo *invariante* in G; allora Σ coincide con Γ stesso e l'ordine del gruppo complementare $H = \frac{G}{\Gamma}$ è precisamente eguale all'indice di Γ in G. Si vede adunque che: *Se* Γ *è un sottogruppo invariante di* G, *si può sempre costruire un gruppo* H, *il gruppo complementare* $H = \frac{G}{\Gamma}$, *col quale* G *è in isomorfismo meriedrico, all'identità in* H *corrispondendo il sottogruppo* Γ *in* G.

Ritornando al caso generale, osserviamo che insieme al gruppo complementare *a destra* $H = \frac{G}{\Gamma}$ potremmo anche considerare un gruppo complementare *a sinistra* H'; però questi due gruppi, come facilmente si vede, possono sempre porsi in corrispondenza d'isomorfismo oloedrico (all'identità in ciascuno corrispondendo il medesimo sottogruppo Σ in G) e sono quindi, astrattamente considerati, identici. Nel caso particolare poi che sia Γ invariante in G, siccome due sostituzioni equivalenti a destra lo sono anche a sinistra e inversamente, i due gruppi complementari H, H' assolutamente coincidono.

§. 18. — Alla ricerca della *composizione* di un gruppo poniamo a fondamento i due seguenti teoremi. Il primo di essi si enuncia:

A) *Siano* G, G' *due gruppi di sostituzioni sopra lettere, dei rispettivi ordini* m, m' *e fra di loro permutabili nel senso che ciascuno di essi sia permutabile con tutte le sostituzioni dell'altro e il loro sottogruppo comune* Γ *abbia l'ordine* μ. *Combinando fra loro per moltiplicazione tutte le sostituzioni di* G *con tutte quelle di* G', *si otterranno soltanto*

$$\frac{m\,m'}{\mu}$$

sostituzioni distinte, che formeranno un gruppo H, *contenente* G, G' *come sottogruppi invarianti, e* Γ *stesso sarà un sottogruppo invariante di* H.

Siano

$$\gamma_1\ \gamma_2\ ,\ .\ ,\ \gamma_\mu$$

le sostituzioni di Γ, sottogruppo comune di G, G', e posto

$$m = n\,\mu\ ,\quad m' = n'\,\mu\ ,$$

(con n, n' interi), si distribuiscano le sostituzioni di G, G' rispetto a Γ nei due quadri

$$G = (\Gamma,\ \Gamma g_2\ ,\ \Gamma g_3\ , \ldots \Gamma g_n\ )$$
$$G' = (\Gamma,\ \Gamma g'_2\ ,\ \Gamma g'_3\ , \ldots \Gamma g'_{n'}).$$

Ora siano g, g' due sostituzioni qualunque, l'una di G l'altra di G'. La sostituzione

$$(gg') \cdot (g'g)^{-1}$$

si può scrivere nei due modi seguenti

$$(gg')(g'g)^{-1} = (gg'g^{-1}) \cdot g'^{-1}$$
$$(gg') \cdot (g'g)^{-1} = g\,(g'g^{-1}g'^{-1})\ ,$$

e poichè, per le ipotesi fatte, la $gg'g^{-1}$ è in G' e l'altra $g'g^{-1}g'^{-1}$ è in G, vediamo che la sostituzione scritta appartiene sì a G che a G' ed è per ciò una γ, diciamo γ_i. Dunque si ha

1) $$gg' = \gamma_i \cdot g'g;$$

in parole: *Due sostituzioni l'una di* G *l'altra di* G' *sono sempre fra loro permutabili a meno di una sostituzione* γ_i *del loro sottogruppo comune* [1]).

Ora formiamo tutti i possibili prodotti

$$gg'\ ,$$

che sono *formalmente* in numero di mm'.

Ma, per valutare il numero effettivo di questi prodotti diversi, osserviamo che, avendosi

$$g = \gamma_i g_\alpha\ ,\ g' = \gamma_k g'_\beta\ ,$$

sarà

$$gg' = \gamma_i g_\alpha \cdot \gamma_k g'_\beta$$

e poichè, per la 1),

$$g_\alpha \gamma_k = \gamma_i g_\alpha\ ,$$

potremo scrivere

$$gg' = \gamma_i g_\alpha g'_\beta\ .$$

---

[1]) Si noti che nella 1) si può anche porre la γ moltiplicatrice a destra, cangiandone l'indice cioè: $gg' = g'g \cdot \gamma_k$.

Si ottengono già dunque tutti i prodotti distinti gg' nella espressione

2) $$\gamma_l g_\alpha g'_\beta$$

facendo

$$\begin{cases} l = 1, 2, 3 \ldots \mu \\ \alpha = 1, 2, 3 \ldots n \\ \beta = 1, 2, 3 \ldots n'. \end{cases}$$

Ora queste $\mu n n' = \frac{m m'}{\mu}$ sostituzioni 2) sono tutte effettivamente distinte, poichè da

$$\gamma_l g_\alpha g'_\beta = \gamma_i g_a g'_b$$

seguirebbe

$$(\gamma_i g_a)^{-1} \cdot \gamma_l g_\alpha = g'_b g'^{-1}_\beta,$$

onde queste due sostituzioni eguali, appartenendo sì a G che a G', sarebbero in Γ e però $b = \beta$, indi $a = \alpha$, $i = l$. Dunque intanto i prodotti distinti gg' sono in numero di $\frac{mm'}{\mu}$ e dati dalla 2). Dalla 1) risulta poi subito che essi formano un gruppo H, il cui ordine è adunque $\frac{mm'}{\mu}$.

Indicando con

$$h = gg'$$

una qualunque sostituzione di H, si ha inoltre

$$h^{-1} \mathrm{G} h = g'^{-1} g^{-1} \mathrm{G} g g' = g'^{-1} \mathrm{G} g' = \mathrm{G}$$

e similmente

$$h^{-1} \mathrm{G}' h = \mathrm{G}',$$

per cui G, G' sono sottogruppi invarianti di H e tale sarà pure evidentemente il loro sottogruppo comune Γ. Così tutte le parti della proposizione A) sono dimostrate.

Passiamo ora al secondo teorema fondamentale per la teoria della composizione dei gruppi, che si enuncia:

B) *Se un gruppo* Γ *possiede due diversi sottogruppi invarianti massimi* G, G′ [1]), *il loro sottogruppo comune* Σ *è invariante massimo sì in* G *che in* G′ *ed ha, rispetto a* G, *l'indice di* G′ *in* Γ *e, rispetto a* G′, *l'indice di* G *in* Γ.

Intanto poichè G, G′ sono fra loro permutabili, nel senso del teorema A), potremo applicare il teorema stesso e se m, m', μ sono i rispettivi ordini di G, G′, Σ i prodotti

$$gg'$$

saranno in numero di $\frac{mm'}{\mu}$ distinti e formeranno un gruppo H contenente G, G′ come sottogruppi invarianti e contenuto esso stesso in Γ come sottogruppo invariante, perchè, essendo γ una qualunque sostituzione di Γ, si ha che $\gamma^{-1}(gg')\gamma = (\gamma^{-1}g\gamma)(\gamma^{-1}g'\gamma')$ è nuovamente un prodotto gg'.

Dall'ipotesi fatta che G, G′ siano invarianti massimi in Γ segue quindi che H coincide con Γ, cioè: *che ogni sostituzione* γ *di* Γ *è un prodotto* gg' [2]). Dunque Γ è d'ordine $= \frac{mm'}{\mu}$ e però l'indice di G in Γ è dato da $\frac{m'}{\mu}$, come l'indice di Σ in G′, e similmente gli indici di Σ in G o di G′ in Γ sono $= \frac{m}{\mu}$.

Per dimostrare completamente il teorema B) resta solo da provare che Σ, che è invariante in Γ stesso pel teorema A), è invariante massimo in G ed in G′. Dimostriamo p. e. che è invariante massimo in G. Sia, se è possibile, Δ un sottogruppo (puro) di G, invariante in G e contenente Σ, e indichiamo con δ le sostituzioni di Δ.

Per la 1), essendo le δ parte delle g, si ha

$$\delta g' = \sigma_i g' \delta,$$

---

[1]) Per chiarire come un gruppo Γ possa contenere due diversi sottogruppi invarianti massimi, si consideri l'esempio seguente. Essendo p, q, r tre numeri primi diversi, si prenda una sostituzione S a periodo $p.q.r$ e si consideri il gruppo ciclico Γ delle potenze di S, indi i due sottogruppi G, G′ generati rispettivamente da S^p, S^q che saranno invarianti massimi in Γ d'indici p, q.

[2]) Si osservi che la conclusione $H = \Gamma$ vale anche se uno soltanto dei sottogruppi G, G′ è invariante massimo in Γ, purchè naturalmente non contenga l'altro come sottogruppo.

indicando σ_i una sostituzione di Σ, onde segue

$$g'^{-1}\,\delta\,g' = (g'^{-1}\,\sigma_i\,g')\,\delta = \sigma_k\,\delta = \delta'.$$

Dunque Δ è permutabile con tutte le g', come evidentemente G' è permutabile con tutte le δ e poichè Δ è permutabile anche colle g, sarà invariante in Γ stesso.

Se indichiamo dunque con $k\,\mu$ l'ordine di Δ, ove k sarà un divisore di $\frac{m}{\mu}$, ed applichiamo il teorema A) stesso, osservando che il sottogruppo comune a G', Δ è ancora Σ, vediamo che i prodotti

$$\delta\,g',$$

in numero di $\frac{k\,\mu\,.\,m'}{\mu} = k\,m'$, formerebbero un gruppo Λ contenente G' e che sarebbe invariante in Γ, poichè

$$\gamma^{-1}\,(\delta\,g')\,\gamma = (\gamma^{-1}\,\delta\,\gamma)\;(\gamma^{-1}\,g'\,\gamma)$$

è nuovamente un prodotto $\delta\,g'$. Per l'ipotesi che G' sia invariante massimo in Γ, dovrà dunque Λ coincidere con Γ, quindi Δ con G [1]).

§. 19. — Sia G un gruppo, G_1 un sottogruppo invariante massimo di G, indi G_2 un sottogruppo invariante massimo di G_1, medesimamente G_3 un sottogruppo invariante massimo in G_2 e così via, finchè si arrivi alla identità. La serie di gruppi

3) $$G,\ G_1,\ G_2,\ G_3 \ldots G_{\mu-1},\ 1,$$

così formata (a cominciare dal gruppo dato G) che ciascun gruppo della serie sia invariante massimo nel precedente, dicesi una *serie di composizione* del gruppo G. Diciamo subito che in generale, per un dato gruppo, si possono formare in molti modi serie diverse di composizione. Se indichiamo poi con

$$m,\ m_1,\ m_2,\ m_3 \ldots m_{\mu-1}\quad 1$$

---

[1]) Si vede che per concludere che Σ è invariante massimo in G basta che G' lo sia in Γ (e non contenga G).

i successivi ordini dei gruppi della serie 3), i quozienti interi

$$e_1 = \frac{m}{m_1} \quad e_2 = \frac{m_1}{m_2}, \ldots e_\mu = m_{\mu-1},$$

che sono gli indici di ciascun gruppo nel precedente, diconsi i *fattori di composizione* del gruppo. Evidentemente si ha

$$m = e_1 e_2 e_3 \ldots e_\mu ,$$

cioè l'ordine del gruppo è il prodotto dei suoi fattori di composizione. JORDAN ha riconosciuto in effetto che questi numeri dipendono unicamente dalla struttura del gruppo e non dalla speciale serie di composizione, dimostrando l'importante teorema:

In due diverse serie di composizione di un medesimo gruppo i fattori di composizione, prescindendo dall'ordine, sono i medesimi.

Dimostreremo il teorema ammettendo che sia vero per tutti i gruppi d'ordine $< m$ e dimostrando che sarà vero anche pei gruppi d'ordine m. Siccome pei primi ordini $m = 2, 3, 4$ [1]) il teorema si verifica immediatamente, così sussisterà in generale.

---

[1]) Per $m = 2, 3$, come in generale per m primo qualunque, un gruppo d'ordine m è necessariamente un gruppo ciclico generato da una sostituzione (operazione) a periodo m e non ha altri sottogruppi che l'identità e però l'unica serie di composizione G, 1.

Per $m = 4$ il gruppo può essere ciclico o no.

Se è ciclico, si ha

$$G_4 = (1, S, S^2, S^3) \quad S^4 = 1$$

e l'unico sottogruppo (oltre l'identità) è

$$\Gamma = (1, S^2)$$

e si ha ancora un'unica serie di composizione.

Se il G_4 non è ciclico, le sue tre operazioni non identiche s_1, s_2, s_3 sono a periodo 2 e si ha

$$s_1 s_2 = s_2 s_1 = s_3 , \; s_1 s_3 = s_3 s_1 = s_2 , \; s_2 s_3 = s_3 s_2 = s_1 .$$

Allora

$$G_4 = (1, s_1, s_2, s_3)$$

ammette i tre diversi sottogruppi invarianti

$$G_1 = (1, s_1) , \; G_2 = (1, s_2) , \; G_3 = (1, s_3) ,$$

quindi tre diverse serie di composizione, nelle quali però i fattori di composizione sono sempre 2, 2. Il gruppo Γ_4 isomorfo a G_4 di sostituzioni su 4 lettere (§. 15) è il gruppo

$$\Gamma_4 = \big(1, (ab)(cd), \; (ac)(bd), \; (ad)(bc) \big) .$$

Supponiamo ora che sia

4) $$G\, G'_1\, G'_2 \ldots G'_{\nu-1}\, 1$$

una nuova serie di composizione di G e siano

$$e'_1,\ e'_2,\ e'_3 \ldots e'_\nu$$

i fattori rispettivi di composizione. Essendo G_1, G'_1 invarianti massimi in G, se indichiamo con Σ il loro sottogruppo comune e con

$$\sum,\ \sum_1,\ \sum_2, \ldots 1$$

una serie di composizione di Σ, le due nuove serie

3*) $$G,\ G_1,\ \sum,\ \sum_1,\ \sum_2, \ldots 1$$

4*) $$G,\ G'_1,\ \sum,\ \sum_1,\ \sum_2, \ldots 1$$

saranno, pel teorema fondamentale B), serie di composizione di G e, pel teorema stesso, i due primi fattori di composizione in 3*) saranno

$$e_1,\ e'_1,$$

invece in 4*)

$$e'_1,\ e_1.$$

Ma, poichè da Σ in poi le 3*) 4*) coincidono, è evidente che: *le due serie di composizione* 3*) 4*) *hanno i medesimi fattori di composizione.* D'altronde se confrontiamo 3) con 3*):

3) $$G,\ G_1,\ G_2,\ G_3 \ldots 1$$

3*) $$G,\ G_1,\ \sum,\ \sum_1 \ldots 1,$$

vediamo che esse hanno i primi due gruppi comuni e, siccome G_1 ha un ordine $< m$, per le ipotesi fatte, i medesimi fattori di composizione.

Lo stesso vale per le serie 4) 4*), onde segue appunto che 3) 4) hanno i medesimi fattori di composizione c. d. d.

Come corollario del teorema di Jordan, si osservi che in due diverse serie di composizione di un medesimo gruppo, il numero dei gruppi nelle due serie è lo stesso.

§. 20. — Siano G, Γ due gruppi oloedricamente isomorfi. Ad ogni sottogruppo Γ_1 di Γ corrisponde un sottogruppo G_1 del medesimo ordine

in G e viceversa; se Γ_1 è invariante in Γ, G_1 sarà invariante in G ed è pur chiaro che se Γ_1 è invariante massimo in Γ, tale sarà pure G_1 in G. Se dunque

$$\Gamma, \Gamma_1, \Gamma_2 \ldots 1$$

è una serie di composizione di Γ e

$$G, G_1, G_2 \ldots 1$$

sono i corrispondenti gruppi in G, questi formeranno una serie di composizione di G. Dunque: *Due gruppi oloedricamente isomorfi hanno i medesimi fattori di composizione.*

Supponiamo ora invece che G sia in isomorfismo meriedrico di grado n con Γ e sia

$$\sum = (\sigma_1 \, \sigma_2 \ldots \sigma_n)$$

il sottogruppo (invariante) di G che corrisponde all'identità in Γ. Riprendendo le considerazioni del §. 14 e distribuendo le sostituzioni di G rispetto a Σ nel quadro

$$G = \left\{ \begin{array}{l} \sum \\ \sum t_2 \\ \vdots \\ \sum t_q, \end{array} \right.$$

vediamo che ad un sottogruppo Γ_1 invariante in Γ corrisponderà in G un sottogruppo G_1 d'eguale indice, invariante in G. Di più se Γ_1 è invariante massimo in Γ, tale sarà anche G_1 in G, poichè un sottogruppo $\bar{G}_1$ di G contenente G_1 consta necessariamente di un certo numero di orizzontali del quadro e, se $\bar{G}_1$ fosse invariante in G, il sottogruppo corrispondente $\bar{\Gamma}_1$ di Γ conterrebbe Γ_1 e sarebbe invariante in Γ.

Ciò premesso, se indichiamo con

$$\Gamma, \Gamma_1, \Gamma_2 \ldots 1$$

una serie di composizione di Γ, e con

$$G, G_1, G_2, \ldots \Sigma$$

indichiamo i corrispondenti sottogruppi in G e completiamo quest'ultima

serie con una serie di composizione di Σ, avremo una serie di composizione di G:

$$G, G_1, G_2, \ldots \sum, \sum_1, \sum_2 \ldots 1 .$$

Concludiamo dunque:

Se il gruppo G *è in isomorfismo meriedrico con* Γ *e all'identità in* Γ *corrisponde il sottogruppo* Σ *in* G, *i fattori di composizione di* G *risultano associando a quelli di* Γ *tutti quelli di* Σ.

§. 21. — Un complemento essenziale al teorema di Jordan è stato arrecato da Hölder [1]), come ora brevemente esponiamo.

Sia

$$3) \qquad G, G_1, G_2, G_3 \ldots 1$$

una serie di composizione del gruppo G, e si considerino i gruppi complementari

$$H_1 = \frac{G}{G_1}, \; H_2 = \frac{G_1}{G_2}, \; H_3 = \frac{G_2}{G_3} \ldots$$

di ciascun gruppo della serie rispetto al successivo. Essendo G_1 invariante massimo in G, il gruppo H_1 è un gruppo *semplice* [2]) d'ordine eguale al primo fattore di composizione di G nella serie 3); analogamente dicasi pei successivi gruppi

$$H_2, H_3 \ldots$$

Chiameremo con Hölder $H_1, H_2, H_3 \ldots$ i gruppi *fattoriali* nella serie di composizione 3). Introdotta la nozione di gruppi fattoriali, il teorema di Jordan si può enunciare così: *In due diverse serie di composizione del medesimo gruppo gli ordini dei gruppi fattoriali corrispondenti sono i medesimi.*

Ora Hölder ha osservato che non soltanto gli *ordini* dei gruppi fattoriali, ma i gruppi fattoriali stessi non fanno che permutarsi fra loro

---

[1]) *Mathem. Annalen,* Bd. 34.

[2]) Si ricordi che G è isomorfo con H_1, all'identità in H_1 corrispondendo G_1 in G. Se H_1 ammettesse un sottogruppo invariante, il corrispondente in G sarebbe pure invariante e conterrebbe G_1.

al cangiare della serie di composizione, cioè: *Se si considerano i gruppi fattoriali*

$$H_1 H_2 \ldots H_\mu$$

$$H'_1 H'_2 \ldots H'_\mu$$

di due diverse serie di composizione di un gruppo, ciascuno dei gruppi H *è oloedricamente isomorfo ad uno dei gruppi* H'.

Per dimostrare questo terema di Hölder basta riprendere il teorema fondamentale B) del §. 18 e completarlo come segue:

B*) *Se un gruppo* Γ *possiede due diversi sottogruppi invarianti massimi* G, G', *il cui sottogruppo comune sia* Σ, *nelle due serie di composizione*

$$\Gamma, G, \sum \ldots$$

$$\Gamma, G', \sum \ldots$$

saranno identici (oloedricamente isomorfi) i due gruppi fattoriali

$$\frac{\Gamma}{G}, \frac{G'}{\sum},$$

come pure gli altri due

$$\frac{\Gamma}{G'}, \frac{G}{\sum}.$$

E infatti, se $\sigma_1, \sigma_2 \ldots \sigma_\mu$ sono le sostituzioni di Σ, distribuendo le sostituzioni di G, G' rispetto a Σ si avrà (§. 18):

$$G = (\sum, \sum g_2, \sum g_3, \ldots \sum g_n)$$

$$G' = (\sum, \sum g'_2, \sum g'_3, \ldots \sum g'_{n'})$$

e, poichè ogni sostituzione di Γ è un prodotto

$$\sigma_\alpha g_i g'_k,$$

distribuendo le sostituzione di Γ rispetto a G o a G' si avrà

$$\Gamma = (G, G g'_2, G g'_3, \ldots G g'_{n'})$$

$$\Gamma = (G', G' g_2, G' g_3, \ldots G' g_n)$$

Così le n sostituzioni

$$g_1 = 1, g_2, g_3 \ldots g_n$$

formeranno un sistema completo di rappresentanti sia di G rispetto a Σ, sia di Γ rispetto a G'. Inoltre se il prodotto $g_i g_k$ è equivalente a g_l rispetto a Σ, lo sarà anche rispetto a G' ed inversamente, e però i due gruppi $\frac{G}{\Sigma}$, $\frac{\Gamma}{G'}$ sono oloedricamente isomorfi; lo stesso dicasi di $\frac{G'}{\Sigma}$, $\frac{\Gamma}{G}$.

Dimostrato il teorema B*), se ne deduce evidentemente il teorema di Hölder, nello stesso modo come al §. 19 abbiamo dedotto il teorema di Jordan dal teorema B) §. 18.

§. 22. — Ritornando al modo di formazione di una serie di composizione per un gruppo dato G, osserviamo che: *Se* G_ν *è un sottogruppo invariante di* G, *esisterà sempre una serie di composizione di* G *che conterrà fra i suoi gruppi* G_ν.

Sia infatti G_1 un sottogruppo invariante massimo di G contenente G_ν, indi G_2 un sottogruppo invariante massimo di G_1, contenente ancora G_ν, e così via finchè si arriva a G_ν stesso. La serie

$$G, G_1, G_2 \ldots G_\nu$$

sarà il principio di una serie di composizione di G, che si potrà completare con una serie di composizione di G_ν [1]).

In una serie di composizione di G avverrà, in generale, che un gruppo intermedio sarà bensì invariante nel precedente, ma non in G. Però possiamo anche formare una serie

$$(5) \qquad G, H, I, K, \ldots 1$$

---

[1]) Evidentemente si potrebbe procedere anche così:

Si costruisca il gruppo complementare $\frac{G}{G_\nu} = H$, col quale G, è in isomorfismo meriedrico, all'identità in H corrispondendo G_ν in G, e sia

$$H, H_1, H_2, \ldots 1$$

una serie di composizione di H. I gruppi corrispondenti $G, G_1, G_2 \ldots G_\nu$ formano i primi termini da G a G_ν della serie di composizione domandata.

così costituita che ciascun gruppo sia sottogruppo del precedente ed invariante in G, ma non si possa fra due gruppi intermedii, p. e. I, K, inserire un sottogruppo di I invariante in G e contenente K.

Una tale serie (5) dicesi una *serie principale* di composizione di G. È chiaro come da una serie principale (5) possa formarsi un'ordinaria serie di composizione

$$(6) \qquad G, H, H_1, H_2 \ldots H_\nu, I, I_1, I_2 \ldots I_\mu, K \ldots,$$

inserendo fra due gruppi consecutivi una serie di composizione del primo gruppo, che contenga il secondo. Ora sussiste il teorema:

Se fra due gruppi consecutivi della serie principale (5), *p. e.* H, I, sono *inseriti i gruppi*

$$H_1, H_2 \ldots H_\nu$$

per formare la serie ordinaria di composizione (6), *i fattori di composizione da* H *fino a* I *sono tutti fra loro eguali.*

Per dimostrarlo basterà, pel teorema di Jordan, dedurre da (5) una serie di composizione come (6), nella quale la detta circostanza si verifichi.

Ora osserviamo che, essendo H_1 invariante in H ma non in G, se trasformiamo H_1 con tutte le sostituzioni di G, otterremo un certo numero di gruppi distinti

$$(7) \qquad H_1, H'_1, H''_1, H'''_1 \ldots,$$

i quali tutti saranno, come H_1, sottogruppi invarianti massimi in H e conterranno I, perchè I è trasformato in se stesso da tutte le sostituzioni di G. Inoltre i gruppi (7) non avranno alcun' altra sostituzione comune all'infuori di quelle di I, poichè, trasformati simultaneamente con una sostituzione di G, essi non fanno che permutarsi fra loro e quindi il loro sottogruppo comune Λ, che contiene I, è invariante in G e contenuto in H e però coincide con I.

Prendiamo due dei gruppi (7) p. e. H_1, H'_1 e sia H_2 il loro sottogruppo comune; potremo cominciare la serie di composizione da H a I con

$$(8) \qquad H, H_1, H_2 \ldots . I,$$

o con

$$(9) \qquad H, H'_1, H_2 \ldots I,$$

e il teorema fondamentale B) §. 18 dimostra che i due primi fattori di composizione nelle (8) (9) sono eguali fra loro, talchè se H_2 coincidesse con I il teorema sarebbe già verificato. Se H_2 non coincide con I, prendiamo fra i gruppi (7) un terzo gruppo H''_1 che non contenga H_2 e sia H_3 il sottogruppo comune di $H_1\ H'_1\ H''_1$ o, ciò che è lo stesso di H_2, H''_1 e così continuiamo finchè si arriva a I, che è il massimo sottogruppo comune dei gruppi (7).

Dobbiamo dimostrare che ciascun gruppo H_r nella serie (8) così costituita è invariante massimo nel precedente H_{r-1} e il fattore di composizione è sempre il medesimo. Per ciò basterà far vedere che, supposta la cosa vera per r gruppi, è vera anche per $r+1$. Ora essendo H_r il sottogruppo comune ai gruppi

$$H_1\ H'_1 \ldots H_1^{(r-2)}\ H_1^{(r-1)}$$

od anche ai due gruppi

$$H_{r-1}\ ,\ H_1^{(r-1)}\ ,$$

ed H_{r+1} il gruppo comune a

$$H_1\ H'_1 \ldots H_1^{(r-1)}\ H_1^{(r)}\ ,$$

ovvero ai due gruppi

$$H_r\ ,\ H_1^{(r)},$$

indichiamo poi con K_r il sottogruppo comune a

$$H_1\ H'_1 \ldots H_1^{(r-2)}\ H_1^{(r)}\ ,$$

ovvero a

$$H_{r-1}\,.\ H_1^{(r)}.$$

Sarà K_r un sottogruppo *puro* di H_{r-1}, chè, se coincidesse con H_{r-1}, se cioè $H_1^{(r)}$ contenesse H_{r-1} e quindi, a più forte ragione, H_r, anche H_{r+1} coinciderebbe con H_r. Allora, per le ipotesi fatte, nelle due serie di $r+1$ termini

$$H\ H_1\ H_2 \ldots H_{r-1}\ H_r$$

$$H\ H_1\ H_2 \ldots H_{r-1}\ K_r$$

ciascun gruppo è sottogruppo invariante massimo nel precedente, con fattore di composizione sempre lo stesso. Ma, essendo H_{r+1} il sottogruppo comune a H_r, K_r, il teorema B) §. 18 dimostra che la proprietà sussiste anche per la serie prolungata fino ad H_{r+1}

$$H,\ H_1,\ H_2 \ldots H_r\ ,\ H_{r+1}\ ,$$

ciò che dimostra completamente il teorema. Se riprendessimo poi le considerazioni che nel §. 21 ci hanno condotto al teorema di Hölder, facilmente potremmo completare il teorema dimostrato, provando che i gruppi fattoriali intermedii

$$\frac{H}{H_1}, \frac{H_1}{H_2}, \ldots \frac{H_\nu}{I}$$

non soltanto hanno ordini (fattori di composizione) eguali, ma sono tutti oloedricamente isomorfi.

In fine osserviamo che, se in una serie principale di composizione

$$G, H, I \ldots 1$$

si chiamano *fattori principali* di composizione gli indici di ciascun gruppo nel precedente, ne segue, applicando il solito teorema B) §. 18, che in due serie principali diverse si presentano, salvo l'ordine, i medesimi fattori principali.

§. 23. — Quando è dato un gruppo, una delle più importanti ricerche da farsi è quella di esaminarne la composizione. Risolviamo qui una tale questione per il gruppo totale di $\pi(n)$ sostituzioni sopra n lettere; si vedrà poi, nella seconda parte, quale importanza fondamentale ha il problema così risoluto per le questioni che concernono la risolubilità algebrica delle equazioni.

Abbiamo già osservato che il gruppo totale $G_{\pi(n)}$ contiene, come sottogruppo invariante, il gruppo alterno $\Gamma_{\frac{\pi(n)}{2}}$; ora dimostriamo:

Eccettuato il caso $n = 4$, non esiste nel gruppo totale alcun altro sottogruppo invariante all'infuori del gruppo alterno.

Si supponga Γ sottogruppo invariante nel gruppo totale $G_{\pi(n)}$ e Γ non coincida col gruppo alterno. Essendo Γ permutabile con *qualunque* sostituzione sulle n lettere, se contiene una sostituzione γ conterrà anche tutte le sue simili, e però (§. 8) nessuna sostituzione di Γ potrà, decomposta in cicli, constare di un solo ciclo. Ora scegliamo fra le sostituzioni di Γ una sostituzione S non identica, che sposti il minor numero possibile di lettere e sia, decomposta in cicli:

$$S = (ab\ldots)\ (cd\ldots)\ (ef\ldots), \ldots$$

dove, per quanto precede, il numero dei cicli sarà almeno 2. In Γ esisterà anche la sostituzione simile

$$S_1 = (ab\ldots)\ (cd\ldots)^{-1}\ (ef\ldots)^{-1}\ldots,$$

quindi

$$S\,S_1 = (ab\ldots)^2.$$

Questa, se non fosse $(ab\ldots)^2 = 1$, senza essere l'identità, sposterebbe meno elementi di S contro l'ipotesi. Dunque intanto tutti i cicli di S sono del 2.° ordine, cioè

$$S = (ab)\ (cd)\ldots,$$

Ma il numero di questi cicli non può superare 2; perchè, se fosse

$$S = (ab)\ (cd)\ (ef)\ldots,$$

avremmo in Γ anche

$$S_1 = (ac)\ (bd)\ (ef)\ldots$$

e però anche

$$S\,S_1 = (ad)\ (bc)$$

che sposta meno elementi di S. In conseguenza S ha necessariamente la forma

$$S = (ab)\ (cd)$$

e si trovano in Γ tutti i prodotti di due trasposizioni con lettere diverse. Ora, se $n > 4$, vi sarà almeno una 5.ª lettera e, quindi avremo in Γ anche

$$S_1 = (ae)\ (cd)$$

e il prodotto $SS_1 = (abe)$, che sposta meno elementi di S. Così per $n > 4$ il teorema è dimostrato e, siccome per $n = 2, 3$ è di immediata evidenza, è completamente dimostrato quanto è asserito.

Osserviamo poi che, nel caso $n = 4$, le considerazioni superiori dimostrano che un sottogruppo invariante del gruppo totale G_{24}, non coincidente col gruppo alterno, ha soltanto sostituzioni che spostano (l'identità esclusa) tutte quattro le lettere e sono tutti i possibili prodotti di due trasposizioni

$$S_1 = (ab)\ (cd)$$

$$S_2 = (ac)\ (bd)$$

$$S_3 = (ad)\ (bc).$$

Queste, insieme coll'identità, formano effettivamente un sottogruppo invariante del 4.° ordine. Dunque: *Nel caso $n=4$ il gruppo totale* G_{24} *ammette due soli sottogruppi invarianti e cioè il gruppo alterno* Γ_{12} *ed il sottogruppo del 4.° ordine*

$$H_4 = \Big(1, (ab)(cd), (ac)(bd), (ad)(bc)\Big).$$

§. 24. — Resta ora che ricerchiamo la composizione del gruppo alterno; la questione è risoluta dall'importante teorema:

Eccettuato il caso $n=4$, il gruppo alterno è semplice.

Supposto che il gruppo alterno sia composto, siano

$$G_{\pi(n)}, \Gamma_{\frac{1}{2}\pi(n)}, H_m$$

rispettivamente il gruppo totale, il gruppo alterno ed un sottogruppo invariante massimo d'ordine m nel gruppo alterno.

Poichè H è invariante in Γ, ma non in G, trasformando H con una sostituzione dispari t si avrà un nuovo gruppo

$$H_1 = t^{-1} H t,$$

che sarà anch'esso invariante massimo in $\Gamma = t^{-1}\Gamma t$.

Trasformando i due gruppi H, H_1 con una sostituzione qualsiasi g di G, i gruppi

$$g^{-1} H g, \; g^{-1} H_1 g$$

saranno H e H_1 stessi se g è pari, ed invece H_1, H se g è impari.

Indichiamo con Σ il sottogruppo comune ad H, H_1; questo, pel teorema B) §. 18, sarà invariante in Γ ed avrà un ordine

$$\mu = \frac{m^2}{\frac{1}{2}\pi(n)}.$$

Ora si osservi che Σ sarebbe invariante non solo in Γ ma anche in G, poichè

$$g^{-1} \sum g$$

è sottogruppo comune di

$$g^{-1} H g, \; g^{-1} H_1 g,$$

cioè di H, H_1. Pel teorema al §. precedente, sarà dunque $\mu = 1$; si avrà cioè

$$3 \,.\, 4 \,.\, 5 \ldots n = m^2. \tag{10}$$

L'ipotesi che il gruppo alterno non sia semplice ci porterebbe dunque a concludere che $\frac{1}{2}\pi(n)$ dovrebbe essere un quadrato perfetto, ciò che, stando ad un teorema sulla frequenza dei numeri primi [1]), è un risultato assurdo.

Ma, senza ricorrere a questo teorema, si potrà proseguire la dimostrazione nel modo seguente. Certamente per i primi valori di $n > 4$

$$n = 5,\ 6, \ldots$$

il gruppo alterno è semplice, i numeri

$$\frac{1}{2}\pi(5) = 60,\ \frac{1}{2}\pi(6) = 360\ldots$$

non essendo quadrati. Basterà dunque provare che il teorema è vero per $n > 6$ se lo è per $n - 1$. Ora il sottogruppo H supposto è certamente transitivo sulle n lettere; poichè, se prendiamo una sostituzione h di H e la decomponiamo in cicli

$$h = (a\,b \ldots)\ (c\,d \ldots) \ldots,$$

prese due lettere qualunque α, β il gruppo alterno Γ, che è $n - 2 > 4$ volte transitivo, contiene certamente una sostituzione

$$\gamma = \begin{pmatrix} \alpha\beta \ldots \\ a\,b \ldots \end{pmatrix},$$

che porta le lettere ab in $\alpha\beta$; quindi in H, che è invariante in Γ, avremo la sostituzione

$$h_1 = \gamma^{-1} h \gamma = (\alpha\,\beta \ldots) \ldots$$

che porta α in β, onde H è transitivo.

---

[1]) Il teorema cui qui si allude è il seguente:

Se r è intero, fra r e $2r - 2$ evvi almeno un numero primo.

L'assurdo proviene allora da ciò che, preso $r = \left[\frac{n+2}{2}\right]$, un numero primo fra r e $2r - 2$ entrerebbe solo alla prima potenza in $\frac{\pi(n)}{2}$.

Ciò posto, prendiamo una lettera ad arbitrio fra le n p. e. x_1 e consideriamo i sottogruppi Γ_1, H_1 di Γ, H che lasciano fissa x_1; il primo è il gruppo alterno sulle $n-1$ lettere

$$x_2\,,\ x_3 \ldots x_n$$

e il secondo H_1 essendo invariante in Γ_1 si riduce, per ipotesi, all'identità. Dunque H, che è transitivo, ha soltanto la sostituzione identica che lascia ferma x_1 e perciò, secondo il teorema al §. 10, il suo ordine m è $= n$. Allora la (10) diventa

$$3\,.\,4\,.\,5 \ldots n = n^2$$

cioè

$$3\,.\,4\,.\,5 \ldots (n-1) = n\,,$$

risultato evidentemente assurdo, perchè n e $n-1$ sono primi fra loro.

Come risultato finale della nostra ricerca, abbiamo che il gruppo totale per $n > 4$ ha un'unica serie di composizione che consta del gruppo totale, del gruppo alterno e della identità, coi fattori di composizione

$$2,\ \frac{1}{2}\,\pi(n).$$

Lo stesso vale evidentemente per $n = 2, 3$. Pel caso $n = 4$ i primi tre gruppi nella serie di composizione sono necessariamente

$$G_{24}, \Gamma_{12}, H_4 = \Big(1\,,\,(ab)(cd)\,,\ (ac)(bd)\,,\ (ad)(bc)\Big).$$

Con uno dei tre sottogruppi di 2.° ordine di H_4 completiamo la serie di composizione che ha i fattori 2, 3, 2, 2.

§. 25 — Uno dei più importanti teoremi della teoria generale dei gruppi è il *teorema di Sylow*, di cui ci andiamo ora ad occupare, teorema del quale Cauchy aveva fatto conoscere alcuni casi particolari.

L'ordine di ogni sottogruppo è sempre, come sappiamo, un divisore dell'ordine del gruppo. In generale però, preso ad arbitrio un divisore dell'ordine del gruppo, non sempre esistono sottogruppi dell'ordine corrispondente; ma ciò accade certamente, secondo il primo teorema di Sylow, quando questo divisore è la potenza di un numero primo.

Sussiste cioè il teorema: *Se l'ordine m di un gruppo* G *è divisibile per la potenza p^α di un numero primo p, esiste in* G *qualche sottogruppo d'ordine p^α* [1]).

Ammetteremo già dimostrato che ogni gruppo il cui ordine sia divisibile per $p^{\alpha-1}$ ammetta sottogruppi d'ordine $p^{\alpha-1}$ e proveremo che allora esisterà in G qualche sottogruppo d'ordine p^α. Siccome in ogni gruppo esiste certamente l'identità, ne seguirà che G ammette sottogruppi dei varii ordini

$$p, p^2, p^3 \ldots p^\alpha .$$

Consideriamo quelle sostituzioni di G *che sono permutabili con ogni altra sostituzione di* G, fra le quali avremo almeno l'identità; siano

$$\sigma_1 = 1, \sigma_2, \sigma_3 \ldots \sigma_n$$

queste sostituzioni. Esse formano evidentemente in G un sottogruppo Σ, che si dirà il sottogruppo *commutativo* di G.

Ora diciamo *affini* due sostituzioni a, b in un gruppo G quando esiste nel gruppo qualche sostituzione g che trasforma a in b:

$$b = g^{-1} a g ,$$

con che sarà anche

$$a = g b g^{-1}$$

cioè a trasformata di b per mezzo della g^{-1}. Si vede subito che *due sostituzioni affini ad una terza sono affini fra loro;* in simboli da

$$c = g^{-1} a g , \quad c = g_1^{-1} b g_1$$

segue

$$a = g g_1^{-1} b g_1 g^{-1} = (g_1 g^{-1})^{-1} b (g_1 g^{-1}) .$$

Ne segue che possiamo ripartire le sostituzioni di G in classi di sostituzioni affini, ponendo nella medesima classe tutte quelle che sono affini ad una stessa, indi fra loro. Se da ogni classe si estrae, ad arbitrio, una sostituzione si formerà un *sistema completo* di sostituzioni non affini, nel senso che ogni altra sostituzione di G sarà affine ad una e ad una sola fra queste. Ciascuna sostituzione σ del gruppo commutativo

---

[1]) La dimostrazione data nel testo è quella di Frobenius (*Crelle's Journal* Bd. 100).

forma per sè sola una classe; ma ciò non avviene per alcun'altra sostituzione del gruppo. Ciò posto sia

$$\text{(A)} \qquad \sigma_1, \sigma_2 \ldots \sigma_n, g_1 g_2 \ldots g_\nu$$

un sistema completo di sostituzioni non affini di G e indichiamo rispettivamente con

$$q_1, q_2, \ldots q_\nu$$

il numero delle sostituzioni nelle rispettive classi di

$$g_1, g_2 \ldots g_\nu \;;$$

avremo evidentemente

$$\text{(11)} \qquad m = n + q_1 + q_2 + \ldots + q_\nu \,.$$

Valutiamo ora in modo preciso i numeri q, ciascuno dei quali, per quanto sopra è detto, è certamente > 1. Prendasi ad esempio la sostituzione g_i. Quelle sostituzioni di G che trasformano g_i in sè medesima (che sono permutabili con g_i) formano in G un sottogruppo G_i il cui ordine indichiamo con m_i; questo gruppo G_i contiene evidentemente il sottogruppo commutativo Σ ed è contenuto come puro sottogruppo in G, cioè $m_i < m$. È facile provare che si avrà allora precisamente

$$q_i = \frac{m}{m_i} \,.$$

Se distribuiamo infatti le sostituzioni del gruppo G rispetto a quelle di G_i nel quadro

$$G = \left\{ \begin{array}{l} G_i \\ G_i t_2 \\ G_i t_3 \\ \vdots \\ G_i t_{\frac{m}{m_i}} \end{array} \right. ,$$

vediamo subito che due sostituzioni di G trasformano g_i nella medesima sostituzione se si trovano nella medesima orizzontale e invece in sostizioni diverse se appartengono a differenti orizzontali. Dunque il numero q_i delle sostituzioni affini a g_i eguaglia il numero delle orizzontali, cioè $\frac{m}{m_i}$. Dopo ciò la (11) si scrive

$$\text{(12)} \qquad m = n + \frac{m}{m} + \frac{m}{m_2} + \ldots + \frac{m}{m_\nu}$$

e da questa relazione possiamo ora dedurre il teorema di SYLOW. Per ciò faremo vedere che l'ipotesi che G non contenga alcun sottogruppo d'ordine p^α conduce ad un risultato assurdo.

Distinguiamo due casi, secondo che l'ordine n del sottogruppo commutativo è divisibile, o non divisibile per p.

1.° *caso: n divisibile per p.* Allora cominciamo dal dimostrare che vi è in Σ qualche sostituzione a periodo p. Indicando con

$$\beta_1 = 1, \beta_2, \beta_3 \ldots \beta_n$$

i rispettivi periodi di

$$\sigma_1, \sigma_2, \sigma_3 \ldots \sigma_n$$

si costruiscano i seguenti $\beta_1 \beta_2 \beta_3 \ldots \beta_n$ prodotti:

$$\sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \sigma_3^{\alpha_3} \ldots \sigma_n^{\alpha_n}, \tag{13}$$

gli esponenti α_i percorrendo sistemi completi di resti rispetto ai moduli β_i p. e.

$$\begin{cases} \alpha_1 = 0, 1, 2 \ldots \beta_1 - 1 \\ \alpha_2 = 0, 1, 2 \ldots \beta_2 - 1 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \alpha_n = 0, 1, 2 \ldots \beta_n - 1. \end{cases}$$

I prodotti (13) danno tutte e sole le n sostituzioni σ; ma ciascuna σ si trova ripetuta in (13) il medesimo numero q di volte, quante volte cioè riesce

$$\sigma_2^{\alpha_1} \sigma_2^{\alpha_2} \ldots \sigma_n^{\alpha_n} = 1,$$

come subito si vede per la permutabilità due a due delle σ. Si avrà quindi

$$\beta_1 \beta_2 \ldots \beta_n = qn$$

e, siccome n è divisibile pel numero primo p, una almeno delle β, poniamo β_i, sarà divisibile per p. La sostituzione di Σ

$$\sigma = \sigma_i^{\frac{\beta_i}{p}}$$

sarà quindi precisamente a periodo p, come si voleva. Consideriamo allora il gruppo ciclico d'ordine p

$$\Gamma = (1, \sigma, \sigma^2, , \ldots \sigma^{p-1})$$

che è sottogruppo *invariante* in G e costruiamo il gruppo complementare

$$H = \frac{G}{\Gamma},$$

che sarà d'ordine $= \frac{m}{p}$; il gruppo G sarà in isomorfismo meriedrico di grado p con H.

Ora l'ordine $\frac{m}{p}$ di H essendo divisibile per $p^{\alpha-1}$ avremo, per ipotesi, in H almeno un sottogruppo d'ordine $p^{\alpha-1}$ e a questo corrisponderà in G un sottogruppo d'ordine p^{α}, contro la nostra ipotesi.

Resta da considerarsi il 2.° caso: *n non divisibile per p.* Allora, per la (12), uno almeno dei numeri $\frac{m}{m_i}$ non deve contenere il fattore p. In tal caso il corrispondente ordine $m_i < m$ di G_i è evidentemente divisibile esso stesso per p^{α}. Dunque: *Se* G *non contiene alcun sottogruppo d'ordine p^{α}, esiste in* G *almeno un sottogruppo (puro)* G_i, *il cui ordine $m_i < m$ è divisibile ancora per p^{α}.*

Nella nostra ipotesi non potrà nemmeno G_i contenere un sottogruppo d'ordine p^{α}, onde pel risultato sopra ottenuto esisterà un divisore puro m'_i di m_i divisibile per p^{α}. Avremmo dunque una serie infinita decrescente di divisori

$$m_i,\ m'_i,\ m''_i \ldots,$$

di m tutti divisibili per p^{α}, ciò che è assurdo.

Dal teorema di Sylow così dimostrato seguono come corollarii i tre teoremi seguenti di Cauchy:

1.° *Se p^{α} è la più alta potenza del numero primo p che divide $\pi(n)$* [1]), *si può formare un gruppo d'ordine p^{α} su n lettere. Tale gruppo contiene sottogruppi degli ordini*

$$p^{\alpha-1},\ p^{\alpha-2} \ldots p\ .$$

2.° *Se l'ordine di un gruppo è divisibile pel numero p, esiste nel gruppo qualche sostituzione a periodo p.*

---

[1]) È noto che questo esponente α è dato da

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^r}\right]$$

quando n sia compreso fra p^r e p^{r+1} (Dirichlet, *Teoria dei numeri).*

Infatti esiste in G qualche sottogruppo Γ d'ordine p ed ogni sostituzione (non identica) di Γ è a periodo p.

§. 26. — Un secondo teorema, egualmente dovuto a SYLOW, riguarda il caso in cui p^α sia la più alta potenza del numero primo p che divide l'ordine m del gruppo G. SYLOW ha dimostrato allora che tutti i sottogruppi d'ordine p^α in G sono trasformati l'uno dell'altro per mezzo di sostituzioni di G e il loro numero q è sempre della forma

$$q = rp + 1.$$

È questo un risultato della massima importanza per la teoria generale dei gruppi; procederemo alla dimostrazione con considerazioni analoghe a quelle che ci hanno servito pel primo teorema. Esiste intanto certamente in G qualche sottogruppo d'ordine p^α ; uno di essi sia H_1 Se trasformiamo H_1 con tutte le sostituzioni di G, otterremo un certo numero q di sottogruppi di G

$$H_1, H_2, \ldots H_q,$$

tutti d'ordine p^α , trasformati di H_1 e quindi l'uno dell'altro. Per valutare questo numero q, consideriamo quelle sostituzioni di G che trasformano H_1 in sè medesimo ; queste formano un sottogruppo Γ di G, contenente H_1 come sottogruppo invariante.

Poniamo per l'ordine m di G

$$m = k\, p^\alpha ,$$

ove k non sarà più divisibile per p, e sia

$$m' = \delta\, p^\alpha$$

l'ordine di Γ, ove δ è un divisore di k.

Se indichiamo con $r = \frac{k}{\delta}$ l'indice di Γ in G e distribuiamo le sostituzioni di G, rispetto a Γ, nel quadro

$$G = \left\{ \begin{array}{l} \Gamma \\ \Gamma g_2 \\ \Gamma g_3 \\ \vdots \\ \Gamma g_r \end{array} \right.$$

vediamo subito che due sostituzioni di G, appartenenti alla medesima orizzontale, trasformano H_1 nel medesimo gruppo e due di orizzontale diversa in gruppi diversi. Per ciò il numero q dei sottogruppi trasformati di H_1 è eguale al numero r delle orizzontali, cioè $q = \frac{k}{\delta}$ e si ha

$$(14) \qquad H_2 = g_2^{-1} H_1 g_2, \; H_3 = g_3^{-1} H_1 g_3 \ldots H_q = g_q^{-1} H_1 g_q .$$

Ciò premesso, enunciamo il secondo teorema di Sylow precisamente così:

Se p^α è la più alta potenza del numero primo p che divide l'ordine m di un gruppo G, *tutti i sottogruppi d'ordine p^α in* G *sono trasformati l'uno dell'altro per sostituzioni di* G. *Il loro numero q eguaglia l'indice in* G *del massimo sottogruppo di* G, *contenente uno dei detti sottogruppi come sottogruppo invariante, e si ha*

$$q \equiv 1 \pmod{p} .$$

Per dimostrare questo teorema cominciamo dall'osservare che *nessuna sostituzione di* Γ, *che non sia in* H_1, *può avere per periodo una potenza di p.* E infatti il gruppo complementare $\frac{\Gamma}{H_1}$ d'ordine $= \delta$, non divisibile per p, non può contenere alcuna sostituzione di periodo divisibile per p. Ora Γ è in isomorfismo meriedrico d'ordine p^α con $\frac{\Gamma}{H_1}$, all'identità in $\frac{\Gamma}{H_1}$ corrispondendo H_1 in Γ, e se una sostituzione γ di Γ fuori di H_1 avesse per periodo una potenza di p, la corrispondente in $\frac{\Gamma}{H_1}$ non sarebbe l'identità ed avrebbe per periodo essa stessa una potenza di p. (§. 14). Ora introduciamo la definizione seguente: Essendo H, H′ due gruppi del medesimo ordine e K un gruppo qualsiasi, diciamo i due gruppi H, H′ *affini* rispetto a K se esiste in K qualche sostituzione k che trasformi H in H′:

$$H' = k^{-1} H k$$

ed allora la k^{-1} trasformerà inversamente H′ in H. È manifesto che due gruppi affini ad un terzo rispetto a K sono anche affini fra loro. Ciò premesso, prendiamo i q gruppi

$$H_1, \; H_2, \; H_3 \ldots H_q$$

e distribuiamoli in *classi di gruppi affini rispetto ad uno di essi p. e.* H_1.

È chiaro che H_1 formerà per sè solo una classe; ma ciò non avverrà di alcun altro dei seguenti. E infatti se, per *qualunque* sostituzione h di H_1, si avesse p. e.

$$h^{-1} H_2 h = H_2 ,$$

ne risulterebbe per la (14)

$$h^{-1} g_2^{-1} H_1 g_2 h = g_2^{-1} H_1 g_2 ,$$

cioè

$$(g_2 h g_2^{-1})^{-1} H_1 (g_2 h g_2^{-1}) = H_1$$

e quindi la $g_2 h g_2^{-1}$, trasformando H, in sè medesimo, apparterrebbe a Γ ed, avendo per periodo una potenza di p, ad H_1 stesso. Ciò dovrebbe valere per qualunque sostituzione h di H_1 e g_2 sarebbe quindi in Γ_1, ciò che non è.

Ora vediamo che in ciascuna delle dette classi (la prima (H_1) esclusa) vi è un numero di gruppi H eguale ad una potenza di p. Prendiamo invero H_i ($i > 1$) e cerchiamo quanti sono i gruppi della sua classe.

Sia H'_1 il sottogruppo di H_1 le cui sostituzioni trasformano H_i in sè medesimo. Distribuendo le sostituzioni di H_1 rispetto al sottogruppo H'_1 vediamo, col solito processo, che nella classe di H_i vi sono precisamente tanti gruppi quante unità sono nell'indice di H'_1 in H_1; ora quest'indice è appunto una potenza p^a di p con esponente $a > 0$. Il numero totale q dei gruppi H_i sarà dunque della forma

$$q = 1 + p^a + p^b + p^c + \dots ,$$

con esponenti a, b, $c \dots$ tutti positivi, il che dimostra intanto la congruenza

$$q \equiv 1 \pmod{p}.$$

Resta solo da dimostrare che nessun altro sottogruppo d'ordine p^α ammette G all'infuori di

$$H_1, H_2, \dots H_q.$$

Anzi dimostreremo più in generale: *Qualunque sottogruppo* K *di* G, *d'ordine eguale a una potenza di p, è necessariamente contenuto in uno dei sottogruppi precedenti.*

Sia infatti K un sottogruppo di G d'ordine $p^\beta \leq p^\alpha$. Ripartiamo i q gruppi H_i in classi di gruppi affini *rispetto a* K. Manifestamente essendo

l'ordine di K una potenza di p, in ogni classe, che non consti di un solo gruppo, ve ne ha ancora un numero eguale a una potenza di p. Ma poichè $q \equiv 1 \pmod{p}$, vi dovrà dunque essere *almeno una* classe contenente un solo gruppo, sia p. e. H_1. Ciò significa che ogni sostituzione h di K trasforma H_1 in se stesso e poichè il periodo di k è una potenza di p sarà k contenuta, per quanto sopra si è visto, in H_1 stesso. Così è completata la dimostrazione del secondo teorema di Sylow.

§. 27. — Per una ragione che conosceremo trattando le applicazioni della teoria dei gruppi [1]), dicesi *risolubile* un gruppo quando tutti i suoi fattori di composizione sono numeri primi. Un esempio notevole di gruppi risolubili l'abbiamo nei gruppi d'ordine eguale alla potenza di un numero primo. Sussiste infatti il teorema: *I fattori di composizione di un gruppo di ordine p^r, essendo p primo, sono tutti eguali a p, quindi in numero di r.*

Siccome ogni fattore di composizione di un tale gruppo è necessariamente una potenza di p, basterà stabilire che nessun fattore di composizione può essere una potenza di un numero primo p diverso da p stesso. Un fattore di composizione di un gruppo è necessariamente anche l'ordine di un gruppo *semplice*, cioè del gruppo fattoriale corrispondente (§. 21), talchè la nostra asserzione equivale all'altra: *Ogni gruppo d'ordine p^r, essendo p numero primo, e $r > 1$ è sempre un gruppo composto.*

Anzi dimostreremo di più che *un tale gruppo* possiede sempre un sottogruppo commutativo Σ (§. 25) diverso dall'identità. Riprendendo infatti le considerazioni che al §. 25 ci hanno servito a dimostrare il primo teorema di Sylow, e in particolare la relazione (12) ivi stabilita, questa assumerà nel caso attuale la forma

$$p^r = n + p^a + p^b + p^c + \dots$$

con $a \geq 1$, $b \geq 1$, $c \geq 1 \dots$ ed n essendo appunto l'ordine del sottogruppo commutativo. Di qui segue che non può essere $n = 1$, ma sarà necessariamente una potenza di p, ciò che dimostra il teorema.

Vi sono altri casi nei quali alla semplice ispezione dell'ordine di un gruppo si può senz'altro concludere che il gruppo è risolubile. Così dal secondo teorema di Sylow discende subito il corollario: *Un gruppo* G

---

[1]) V. §. 81.

di ordine $m = pq$, essendo p, q numeri primi differenti od eguali è un gruppo risolubile. Nel caso $p = q$ ciò è già stato sopra stabilito. Supponiamo ora $p > q$. In G esisterà allora, pel secondo teorema di Sylow, un sottogruppo H d'ordine p, ma uno soltanto, perchè il numero di questi sottogruppi deve essere $\equiv 1$ (mod p) e divisore di q. Dunque H è invariante (massimo) in G e si ha la serie di composizione

$$G, H, 1$$

coi fattori primi di composizione q, p.

Ulteriori teoremi del genere di quelli ora stabiliti sono dovuti a Frobenius [1]), ma noi qui, non occorrendo di ricorrervi nel seguito, ci limiteremo ad enunciarli:

1.° *Ogni gruppo il cui ordine non contiene alcun fattore quadrato è un gruppo risolubile.*

2.° *Ogni gruppo di ordine $p^n q$, essendo p, q numeri primi, è un gruppo risolubile.*

§. 28. — Come si è visto negli esempii del §. precedente, vi sono dei numeri interi che non possono mai figurare come fattori di composizione di gruppi o, ciò che torna lo stesso, come ordini di gruppi semplici. In mancanza di criterii generali che servano a decidere, dato un numero m, se esiste o no qualche gruppo semplice d'ordine m, sono state fatte delle ricerche particolari per gli ordini più bassi. E così Hölder e Cole hanno esaurita la ricerca degli ordini possibili dei gruppi semplici da 1 a 660 ed hanno trovato che, fatta astrazione dai numeri primi, i quali sono sempre ordini possibili di gruppi semplici, esistono gruppi semplici soltanto dei 5 ordini seguenti

$$60, 168, 360, 504, 660$$

ed ogni volta vi è un solo tipo corrispondente. Di questi i due di ordini 60, 360 ci sono già noti come gruppi alterni su 5 o su 6 lettere e gli altri due di ordini 168, 660 incontreremo fra breve come *gruppi modulari.* Noi ci contenteremo qui, per dare un'idea di queste ricerche,

---

[1]) *Sitzungsberichte der Berliner Akademie,* Mai 1893. — V. anche Weber, *Algebra,* T. II, pag. 129.

di riscontrare che per numeri *composti* $m \leq 100$ vi è un solo ordine possibile di un gruppo semplice e cioè $m = 60$.

A fondamento della ricerca poniamo le considerazioni seguenti, che derivano dal secondo teorema di SYLOW. Sia G_m un gruppo *semplice* d'ordine m e sia p^α la più alta potenza del numero primo p che divide m, onde $m = k p^\alpha$ con k non divisibile per p. Poichè G è semplice, il numero q dei sottogruppi H d'ordine p^α in G sarà certamente > 1 e dovrà essere un divisore di k che sia $\equiv 1 \pmod{p}$. Se prendiamo questi q sottogruppi

$$H_1, H_2, \ldots H_q$$

e li trasformiamo contemporaneamente con una medesima sostituzione g di G, i gruppi trasformati

$$g^{-1} H_1 g, g^{-1} H_2 g, \ldots g^{-1} H_q g$$

saranno i gruppi stessi in altro ordine, cioè si produrrà su questi q elementi H una sostituzione

$$\gamma = \begin{pmatrix} g^{-1} H_1 g, & g^{-1} H_2 g, & \ldots & g^{-1} H_q g \\ H_1 & H_2 & \ldots & H_q \end{pmatrix}.$$

Il complesso delle sostituzioni γ forma, come subito si vede, un gruppo Γ transitivo sopra $H_1 H_2 \ldots H_q$ e con questo gruppo Γ il gruppo G deve essere in isomorfismo necessariamente *oloedrico*, perchè G è semplice. Astrattamente considerati, i gruppi G, Γ sono identici. Si noti di più che le sostituzioni di Γ saranno tutte pari perchè, se ve ne fossero anche delle dispari, le pari formerebbero in Γ un sottogruppo invariante d'indice 2.

Si scrivano tutti i numeri composti ≤ 100, tralasciando quelli che, per essere di una delle due forme p^n o pq, non possono figurare certamente come ordini di gruppi semplici. Lasciando da parte l'ordine 60, restano i numeri seguenti

12, 18, 20, 24, 28, 30, 36, 40, 42, 44, 45, 48, 50, 52, 54, 56, 63, 66, 68, 70, 72, 75, 76, 78, 80, 84, 88, 90, 96, 98, 99, 100.

Di questi, fatta eccezione dai numeri

30, 56, 90,

che richiedono qualche maggiore osservazione, si riconosce subito che i

rimanenti non possono essere ordini di gruppi semplici con considerazioni affatto analoghe alle seguenti. Prendasi ad esempio $12 = 3 . 2^2$. Se esistesse un gruppo semplice di questo ordine, esso conterrebbe tre sottogruppi del quarto ordine e sarebbe oloedricamente isomorfo con un gruppo di sostituzioni sopra 3 lettere soltanto, ciò che è assurdo. Così ancora, se esistessero gruppi semplici degli ordini $40 = 8 . 5$, $80 = 16 . 5$ dovrebbero contenere 5 sottogruppi rispettivamente degli ordini 8, 16 ed essere quindi oloedricamente isomorfi con gruppi di sostituzioni pari su 5 lettere; essi sarebbero quindi contenuti nel gruppo alterno su 5 lettere, ciò che è assurdo perchè 40, 80 non sono divisori di 60.

Per riconoscere che non possono esistere gruppi semplici degli ordini

$$30 = 2 . 3 . 5, 56 = 7 . 2^3, 90 = 5 . 2 . 3^2$$

facciamo le osservazioni seguenti:

1.° Un gruppo semplice G_{30} dell'ordine 30 conterrebbe

6 sottogruppi del 5.° ordine
10 „ 3.° „

Ora due gruppi diversi d'ordine primo non possono avere alcuna sostituzione comune fuori dell'identità. Avremmo dunque in G_{30}

$4 \times 6 = 24$ sostituzioni a periodo 5
$2 \times 10 = 20$ „ „ 3,

ciò che pone già in evidenza l'impossibilità, essendo $24 + 20 > 30$.

2.° Un gruppo semplice G_{56} dell'ordine 56 conterrebbe

8 sottogruppi del 7.° ordine
7 „ 8.° „

quindi

$6 \times 8 = 48$ sostituzioni a periodo 7,

che aggiunte alle 8 sostituzioni di un solo sottogruppo dell'8.° ordine, esaurirebbero già le $48 + 8 = 56$ sostituzioni del gruppo.

3.° Un gruppo semplice dell'ordine 90 conterrebbe 6 sottogruppi del 5.° ordine e si potrebbe pensare come un gruppo semplice Γ_{90} transitivo d'ordine 90 su 6 lettere

$$H_1 H_2 H_3 H_4 H_5 H_6 .$$

Le sostituzioni di Γ_{90} che lasciano ferma una lettera formerebbero un sottogruppo G_{15} d'ordine

$$\frac{90}{6} = 15 .$$

D'altronde Γ_{90} contiene certo qualche sostituzione a periodo 2 che, dovendo essere pari, conterrebbe due cicli di due lettere e lascerebbe ferme le altre due. In conseguenza il sottogruppo G_{15} conterrebbe delle sostituzioni a periodo 2, il che è assurdo.

§. 29. — Per quanto abbiamo visto nel §. precedente, di gruppi semplici d'ordine composto $m \leq 100$ non ne possono esistere che per $m = 60$. Ma per quest'ordine esistono effettivamente, come lo dimostra l'esempio del gruppo alterno su 5 lettere. Ora vogliamo provare che è questo l'unico tipo esistente, cioè sussiste il teorema:

Ogni gruppo semplice d'ordine 60 *è oloedricamente isomorfo col gruppo alterno su 5 lettere.*

Un gruppo semplice d'ordine 60 contiene precisamente 6 sottogruppi del 5.° ordine ed è quindi oloedricamente isomorfo con un gruppo Γ_{60} transitivo sopra 6 lettere, con sostituzioni tutte pari. Il gruppo Γ_{60} è quindi un sottogruppo del gruppo alterno G d'ordine 360 sulle 6 lettere. L'indice di Γ in G essendo $\frac{360}{60} = 6$, il gruppo complementare

$$H = \frac{G}{\Gamma}$$

è un gruppo oloedricamente isomorfo a G sulle 6 classi

$$g_1 g_2 \cdots g_6,$$

in cui si ripartiscono le sostituzioni di G rispetto a Γ (§. 17); dunque H è il gruppo alterno sulle 6 lettere $g_1 \ldots g_6$.

Al sottogruppo Γ di G corrisponde in H un sottogruppo H' di egual ordine 60. Le sostituzioni di H' lasciano ferma la classe g_1, cui appartengono le sostituzioni di Γ, e però il gruppo H' è precisamente il gruppo alterno sulle rimanenti 5 lettere g_2, g_3, g_4, g_5, g_6, ciò che dimostra il teorema.

Capitolo III.

Gruppi Abeliani. — Gruppo metaciclico. — Gruppo lineare totale sopra $p+1$ indici e gruppo modulare.

§. 30. — Dopo aver trattato, nei due capitoli precedenti, delle proprietà generali dei gruppi, volgiamoci ora allo studio di gruppi particolari importanti per le applicazioni.

Ci occuperemo in primo luogo di quei gruppi le cui sostituzioni (operazioni) sono a due a due permutabili. Tali gruppi diconsi *Abeliani* e godono di proprietà particolari più semplici dipendenti dalla permutabilità delle loro operazioni.

Sia G un gruppo Abeliano d'ordine m e siano

$$g_1 g_2 g_3 \cdots g_m$$

le sue sostituzioni. Partiamo dalla seguente osservazione fondamentale:

In ogni gruppo Abeliano il periodo del prodotto di più sostituzioni

$$g_1 g_2 \cdots g_k$$

è un divisore del minimo multiplo comune dei singoli loro periodi.

Sia infatti n questo minimo multiplo comune. Per la proprietà commutativa delle attuali sostituzioni si ha

$$(g_1 g_2 \cdots g_k)^n = g_1^n g_2^n \cdots g_k^n = 1,$$

il che dimostra la proprietà.

Aggiungiamo di più che: *Se i periodi $n_1, n_2, \ldots n_k$ delle sostituzioni $g_1 g_2 \ldots g_k$ sono primi a due a due fra loro, il periodo del prodotto $g_1 g_2 \ldots g_k$ sarà il prodotto dei periodi $n_1 n_2 \ldots n_k$.* Basterà evidentemente dimostrare il teorema per due sostituzioni g_1, g_2. Ora se $(g_1 g_2)^n = 1$ si ha $g_1^n = g_2^{-n}$; ma la sostituzione a sinistra ha per periodo un divisore di n_1, quella a destra un divisore di n_2, onde si ha $g_1^n = 1$, $g_2^n = 1$ e però n, essendo multiplo sì di n_1 che di n_2, è multiplo del prodotto $n_1 n_2$.

Applicando i teoremi generali della teoria dei gruppi, in particolare i teoremi di Sylow, troviamo subito delle importanti proprietà dei gruppi Abeliani. Decomponendo l'ordine m del gruppo nei suoi fattori primi, sia

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Pel secondo teorema di Sylow, e pel fatto che ogni sottogruppo di un gruppo Abeliano è invariante nel gruppo, esisterà in G un solo sottogruppo Γ_1 d'ordine $p_1^{\alpha_1}$, uno Γ_2 d'ordine $p_2^{\alpha_2}$ e così via. Formiamo tutti i possibili prodotti

$$(1) \qquad g = \gamma_1 \gamma_2 \ldots \gamma_r$$

di una sostituzione γ_1 di Γ_1 per una γ_2 di $\Gamma_2 \ldots$, per una γ_r di Γ_r. Queste sono tutte evidentemente sostituzioni di g; ma nessuna si trova ripetuta perchè da

$$\gamma'_1 \gamma'_2 \ldots \gamma'_r = \gamma_1 \gamma_2 \ldots \gamma_r$$

seguirebbe

$$(\gamma'_1 \gamma_1^{-1})(\gamma'_2 \gamma_2^{-1}) \ldots (\gamma'_{r-1} \gamma_{r-1}^{-1}) = \gamma_r \gamma'^{-1}_r$$

Ora la sostituzione a destra, appartenendo a Γ_r, ha per periodo una potenza di p_r mentre quella a sinistra, per la proprietà osservata sopra, ha un periodo della forma $p_1^{\beta_1} p_2^{\beta_2} \ldots p_{r-1}^{\beta_{r-1}}$, onde si ha $\gamma_r \gamma'^{-1}_r = 1$ cioè $\gamma_r = \gamma'_r$ e similmente $\gamma'_1 = \gamma_1$, $\gamma'_2 = \gamma_2 \ldots$ Ne risulta che dalla formola (1) si trovano date tutte le $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ sostituzioni di G; e possiamo anche scrivere simbolicamente

$$(2) \qquad G = \Gamma_1 \Gamma_2 \ldots \Gamma_r$$

ed enunciare il teorema:

Ogni gruppo Abeliano, d'ordine composto di potenze di diversi numeri primi, si decompone nel prodotto di sottogruppi Abeliani parziali, i cui ordini sono potenze di numeri primi.

Per il medesimo teorema di Sylow, se

$$p_1^{\beta_1},\ p_2^{\beta_2} \ldots p_r^{\beta_r}$$

sono rispettivamente divisori delle potenze

$$p_1^{\alpha_1}\ p_2^{\alpha_2}, \ldots p_r^{\alpha_r},$$

se cioè

$$\beta_1 \leq \alpha_1,\ \beta_2 \leq \alpha_2, \ldots \beta_r \leq \alpha_r,$$

i gruppi

$$\Gamma_1, \Gamma_2, \ldots \Gamma_r$$

posseggono rispettivamente sottogruppi

$$\Gamma'_1, \Gamma'_2, \ldots \Gamma'_r$$

degli ordini

$$p_1^{\beta_1}, p_2^{\beta_2}, \ldots p_r^{\beta_r}.$$

Allora, se consideriamo il gruppo G′ prodotto di questi sottogruppi parziali:

$$G' = \Gamma'_1 \Gamma'_2 \ldots \Gamma'_r,$$

è chiaro che sarà G′ un sottogruppo di G di ordine

$$n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r},$$

che è un divisore *qualunque* di m. Dunque:

Un gruppo Abeliano possiede sottogruppi di tutti gli ordini, divisori dell'ordine del gruppo.

Così pei gruppi Abeliani viene, in certo modo, invertito il teorema fondamentale (§. 7); è questa, come già si è osservato, una proprietà che non sussiste, in generale, per gli altri gruppi.

Osserviamo in particolare che il gruppo Abeliano G possederà sottogruppi dei rispettivi ordini:

$$\begin{array}{l} p_1^{\alpha_1-1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \\ p_1^{\alpha_1-2} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \\ \qquad p_2^{\alpha_2} \ldots p_r^{\alpha_r} \\ \qquad p_2^{\alpha_2-1} \ldots p_r^{\alpha_r} \\ \qquad \ldots\ldots\ldots \\ \qquad\qquad\qquad p_r, \end{array}$$

onde risulta il teorema:

Ogni gruppo Abeliano è un gruppo risolubile.

§. 31. — Abbiamo stabilite, al §. precedente, le proprietà fondamentali dei gruppi Abeliani, servendoci dei teoremi della teoria generale. Ma possiamo anche stabilire direttamente questi teoremi, nel caso particolare dei gruppi Abeliani, giovandoci delle semplici leggi che governano questi gruppi. Cominciamo dal dimostrare direttamente il teorema:

Se si decompone l'ordine m di un gruppo Abeliano G *nel prodotto di due fattori $m_1 . m_2$ primi fra loro, esistono in* G *due sottogruppi*

$$A = (a_1\, a_2 \ldots a_{m_1})$$
$$B = (b_1\, b_2 \ldots b_{m_2})$$

dei rispettivi ordini m_1, m_2, *tali che si ha*

$$G = A \,.\, B\,,$$

cioè i prodotti

$$a_i\, b_k \begin{cases} i = 1, 2, \ldots m_1 \\ k = 1, 2, \ldots m_2 \end{cases}$$

danno tutte le sostituzioni di G, *ciascuna una sola volta.*

Per dimostrarlo, indichiamo con

$$a_1\,,\ a_2\,,\ a_3 \ldots$$

tutte le sostituzioni di G il cui periodo divide m_1; a causa della prima proprietà osservata al §. precedente, esse formano un sottogruppo A di G, il cui ordine indichiamo provvisoriamente con n_1, ma si dimostrerà $= m_1$.

Similmente il complesso B di quelle sostituzioni

$$b_1\, b_2 \ldots b_{n_2}$$

di G, il cui periodo divide m_2 sarà un sottogruppo di G, il cui ordine n_2 dimostreremo $= m_2$. Intanto vediamo subito che ogni sostituzione g di G è il prodotto di una a per una b. E infatti, poichè m_1, m_2 sono primi fra loro, potrà risolversi in numeri interi r, s l'equazione

$$m_2\, r + m_1\, s = 1$$

e si avrà

$$g = g^{m_2\, r} \,.\, g^{m_1\, s}\,.$$

Ora, essendo

$$(g^{m_2\, r})^{m_1} = 1\,,\ (g^{m_1\, s})^{m_2} = 1,$$

si vede appunto che $g^{m_2\, r}$ è una a e $g^{m_1\, s}$ è una b; avremo cioè

$$g = a_i\, b_k\,.$$

Ora questi $n_1\, n_2$ prodotti $a_i\, b_k$ sono differenti fra loro, poichè da

$$a_i\, b_k = a_j\, b_h$$

segue

$$a_i\, a_j^{-1} = b_h\, b_k^{-1}\,,$$

onde $a_i = a_j$, $b_l = b_k$. Avremo quindi

$$m = n_1\, n_2 = m_1\, m_2\,.$$

Ma n_1 è primo con m_2 perchè, se p fosse un loro divisore primo comune, si avrebbe in A una sostituzione a periodo p divisore di m_2 e quindi anche appartenente a B; similmente n_2 è primo con m_1, onde segue

$$n_1 = m_1, \; n_2 = m_2 \quad \text{c. d. d.}$$

Applicando ripetutamente il teorema ora dimostrato, è chiaro come si perviene alla medesima decomposizione (2) del gruppo Abeliano G nel prodotto di gruppi parziali, che nel §. precedente abbiamo dedotto dal teorema di Sylow, e da questa decomposizione possiamo nuovamente trarre tutte le conseguenze ivi osservate.

§. 32. — Nel gruppo Abeliano G prendiamo r sostituzioni

$$g_1, g_2, \ldots g_r;$$

le diremo fra loro *indipendenti* se nessuna sostituzione composta di queste

$$g_1^{s_1} g_2^{s_2} \ldots g_r^{s_r}, \tag{3}$$

può essere l'identità, salvo quando si abbia separatamente

$$g_1^{s_1} = 1, g_2^{s_2} = 1, \ldots g_r^{s_r} = 1,$$

cioè $s_1, s_2, \ldots s_r$ siano rispettivamente multipli dei periodi

$$\beta_1, \beta_2 \ldots \beta_r$$

delle sostituzioni

$$g_1 g_2 \ldots g_r.$$

Se $g_1, g_2, \ldots g_r$ sono fra loro indipendenti, le sostituzioni (3), quando agli esponenti $s_1, s_2 \ldots s_r$ si faccia rispettivamente percorrere un sistema completo di resti rispetto ai moduli

$$\beta_1, \beta_2 \ldots \beta_r,$$

daranno evidentemente un sottogruppo H di G, precisamente di ordine

$$n = \beta_1 \beta_2 \ldots \beta_r.$$

Questo gruppo H si indicherà anche, ponendo in evidenza le sostituzioni generatrici, col simbolo

$$\mathrm{H} = [g_1, g_2, \ldots g_r].$$

Ci proponiamo ora di dimostrare che per ogni gruppo Abeliano si può scegliere un sistema di sostituzioni *generatrici* fra loro indipendenti; un tale sistema si dirà una *base* del gruppo.

A tale oggetto premettiamo le osservazioni seguenti:

a) Se n_1 è il massimo periodo delle sostituzioni di G, *ogni altro periodo è un divisore di n_1.*

Sia g una sostituzione di G del massimo periodo n_1 e g' un'altra sostituzione di G a periodo n_2. Supponiamo che n_2 non divida, se è possibile, n_1 e vi sia per conseguenza almeno un fattore primo p di n_2 che entri in n_2 ad una potenza maggiore che in n_1; poniamo

$$n_1 = n'_1 p^\alpha \ , \ n_2 = n'_2 p^\beta \ ,$$

essendo n'_1, n'_2 non divisibili per p e inoltre $\alpha < \beta$. Le sostituzioni

$$g^{p^\alpha} \ , \ g'^{n'_2}$$

hanno i rispettivi periodi n'_1, p^β primi fra loro e quindi (§. 39) la sostituzione loro prodotto ha il periodo $n'_1 p^\beta > n_1$, ciò che contraddice l'ipotesi.

Consideriamo un sottogruppo qualsiasi H di G. Diremo *periodo relativo* di una sostituzione di g, rispetto ad H, il minimo esponente positivo α cui bisogna elevare g perchè g^α appartenga ad H. Si vede subito che se si costruisce il gruppo complementare $\Gamma = \frac{G}{H}$, che è esso stesso un gruppo Abeliano, il periodo relativo di una sostituzione di G non è altro che il periodo effettivo della corrispondente sostituzione in Γ. Ne risultano subito le proprietà seguenti:

b) Il periodo relativo è sempre un divisore del periodo assoluto.

E infatti se β è il periodo assoluto, a $g^\beta = 1$ corrisponde in Γ l'identità.

c) Due sostituzioni di G *equivalenti rispetto ad* H *hanno il medesimo periodo relativo.*

Ciò è evidente, perchè a due tali sostituzioni di G corrisponde la medesima in Γ.

d) Se n è il massimo periodo relativo di una sostituzione di G, *ogni altro periodo relativo è un divisore di n.*

Questa proprietà risulta subito dall'applicare il teorema *a*) al gruppo complementare Γ.

§. 33. — Premesse queste osservazioni, procediamo alla costruzione effettiva di una base del gruppo Abeliano nel modo seguente. Prendiamo in G una sostituzione g_1 del *massimo* periodo n_1 e costruiamo il sottogruppo ciclico

$$\Gamma = (1, g_1, g_1^2, \ldots g_1^{n_1-1}).$$

Il periodo relativo di ogni sostituzione di G sarà sempre, per quanto abbiamo visto sopra (*a*) *c*) §. 32), un divisore di n_1. Sia n_2 il massimo di questi periodi relativi che sarà un divisore di n_1, senza escludere che possa aversi $n_2 = n_1$, e del quale (§. 32) ogni altro periodo relativo sarà divisore. Dimostriamo che esiste in G almeno una sostituzione g_2 a periodo *assoluto* n_2, o ciò che torna lo stesso, che vi ha in G una sostituzione g_2 indipendente da g_1. A tale scopo prendiamo una sostituzione g a periodo relativo n_2, talchè si avrà

$$g^{n_2} = g_1^{k_1},$$

onde

$$g^{n_1} = g_1^{k_1 \frac{n_1}{n_2}} = 1.$$

L'esponente $k_1 \dfrac{n_1}{n_2}$ deve quindi essere multiplo di n_1, cioè $\dfrac{k_1}{n_2}$ intero. Se sostituiamo allora a g la sostituzione equivalente (rispetto a Γ)

$$g_2 = g \cdot g_1^{-\frac{k}{n_2}},$$

vediamo che g_2 avrà appunto per periodo assoluto n_2, come si voleva.

Mediante le due sostituzioni generatrici indipendenti g_1, g_2 costruiamo il sottogruppo

$$\mathrm{H} = [g_1, g_2]$$

d'ordine $n_1 n_2$. Potremo ora trovare in G una sostituzione g_3 indipendente da g_1, g_2, procedendo in modo perfettamente analogo. Indichiamo perciò con n_3 il massimo periodo relativo delle sostituzioni di G rispetto ad H. Questo numero n_3 è un divisore di n_2, perchè qualunque sostituzione di G, elevata a n_2, trovasi già in Γ; inoltre ogni altro periodo relativo dividerà n_2 (*d*) §. 32). Se g è una sostituzione di G a periodo relativo n_3 rispetto ad H, avremo

$$g^{n_3} = g_1^{k_1} \cdot g_2^{k_2}$$

ed i numeri k_1, k_2 sono divisibili per n_3, come si rileva subito dall'osservare che $g^{n_2} = (g^{n_3})^{\frac{n_2}{n_3}}$ è una potenza di g_1, mentre $g_1^{n_1} = 1$, e ricordando che g_1, g_2 sono indipendenti. Poniamo

$$g_3 = g \,.\, g_1^{-\frac{k_1}{n_3}} \,.\, g_2^{-\frac{k_2}{n_3}}$$

e il periodo *assoluto* di g_3 sarà n_3, poichè $g_3^{n_3} = 1$ ed il suo periodo relativo è $= n_3$.

Le tre sostituzioni g_1, g_2, g_3 sono dunque indipendenti ed il gruppo

$$\mathrm{K} = [g_1, g_2, g_3]$$

è un sottogruppo di G d'ordine $n = n_1 \,.\, n_2 \,.\, n_3$.

Così continuando, stabiliamo evidentemente il teorema seguente:

A) *Per ogni gruppo Abeliano* G *d'ordine m si può trovare una base*

$$[g_1, g_2, g_3 \ldots g_r]$$

dotata delle proprietà seguenti: 1.ª *I periodi*

$$n_1, n_2, \ldots n_r$$

delle rispettive sostituzioni generatrici sono divisori ciascuno del precedente od eguali a questo, ed è $m = n_1 n_2 \ldots n_r$. 2.ª *Ciascun periodo* n_i *di una sostituzione generatrice* g_i *è il massimo periodo relativo delle sostituzioni del gruppo* G *rispetto al sottogruppo* $[g_1, g_2, \ldots g_{i-1}]$ *generato dalle sostituzioni precedenti.*

§. 34. — Nel §. precedente non soltanto abbiamo dimostrata l'esistenza di una base per un gruppo Abeliano, ma abbiamo data alla base del gruppo la forma più appropriata per le applicazioni. Non imponendo alla base alcuna condizione, è facile vedere che si possono costruire basi di un medesimo gruppo con numeri diversi di sostituzioni generatrici e con diversi periodi. Così p. e. per il gruppo Abeliano ciclico generato dalle potenze di una sostituzione S a periodo composto $m = m_1 m_2$, ove m_1, m_2 siano primi fra loro, forma una base la sola sostituzione S, come anche un'altra base è costituita dalle due sostituzioni indipendenti

$$s_1 = \mathrm{S}^{m_2}, \quad s_2 = \mathrm{S}^{m_1},$$

coi rispettivi periodi m_1, m_2.

Ma se costruiamo due diverse basi del gruppo Abeliano G, nel modo del teorema A) al §. precedente, facilmente vediamo che sussiste il teorema:

B) *Due diverse basi*

$$[g_1, g_2, \ldots g_r]$$
$$[g'_1, g'_2, \ldots g'_r]$$

del medesimo gruppo Abeliano, che soddisfino alle condizioni del teorema A), *contengono il medesimo numero di sostituzioni generatrici, coi medesimi periodi.*

Siano

$$n_1, n_2, n_3 \ldots n_r$$

i periodi delle sostituzioni della prima base e

$$n'_1, \; n'_2, \; n'_3 \ldots$$

quelli delle sostituzioni della seconda. Siccome tanto n_1 quanto n'_1 sono il massimo dei periodi delle sostituzioni di G, sarà necessariamente intanto $n'_1 = n_1$. Sarà dimostrato il nostro teorema quando si provi che, supposte le eguaglianze

$$n'_1 = n_1, \; n'_2 = n_2 \ldots n'_{i-1} = n_{i-1},$$

ne segue l'altra $n'_i = n_i$ [1]). Si considerino perciò tutte le sostituzioni di G che sono potenze, con esponenti n_i, di altre sostituzioni del gruppo; queste sostituzioni, che indichiamo con $\bar{g}$, formano evidentemente un sottogruppo di G. Se si pone

$$\bar{g} = g^{n_i}$$

e si esprime g per le sostituzioni della prima base si avrà

$$g = g_1^{\beta_1} g_2^{\beta_2} \ldots g_r^{\beta_r}$$

---

[1]) Si osservi che esistendo una i^{ma} sostituzione g_i ne deve esistere anche una i^{ma} g'_i, altrimenti sarebbe

$$m = n_1 n_2 \ldots n_{i-1} n_i \ldots$$

ed anche

$$m = n_1 n_2 \ldots n_{i-1}.$$

quindi elevando questa eguaglianza all'esponente n_i coll'osservare che

$$g_i^{n_i} = 1\,,\; g_{i+1}^{n_i} = 1 \ldots$$

si avrà

$$\bar{g} = g_1^{\beta_1 n_i}\, g_2^{\beta_2 n_i} \ldots g_{i-1}^{\beta_{i-1} n_i}.$$

Viceversa ogni sostituzione di questa forma è una $\bar{g}$ e però il loro numero è evidentemente dato da $\frac{n_1}{n_i} \times \frac{n_2}{n_i} \times \ldots \times \frac{n_{i-1}}{n_i}$. D'altra parte anche tutte le sostituzioni della forma

$$g'^{\beta_1 n_i}_1\, g'^{\beta_2 n_i}_2 \ldots g'^{\beta_{i-1} n_i}_{i-1}$$

sono evidentemente sostituzioni $\bar{g}$ e il loro numero è il medesimo; dunque ogni sostituzione $\bar{g}$ può anche porsi sotto la forma

$$\bar{g} = g'^{\beta_1 n_i}_1\, g'^{\beta_2 n_i}_2 \ldots g'^{\beta_{i-1} n_i}_{i-1}.$$

Ma fra le sostituzioni $\bar{g}$ vi è pure la $g'^{n_i}_i$ ed, essendo g'_i indipendente da

$$g'_1,\, g'_2, \ldots g'_{i-1}\,,$$

si ha necessariamente $g'^{n_i}_i = 1$. Se ne conclude che n'_i (periodo di g'_i) divide n_i e poichè la considerazione è invertibile si avrà $n'_i = n_i$ c. d. d.

A causa del teorema B), daremo ai numeri $n_1, n_2, \ldots n_r$ il nome di *invarianti* del gruppo Abeliano. L'importante significato inerente a questi numeri risulta dal teorema seguente:

c) *Condizione necessaria e sufficiente perchè due gruppi Abeliani siano oloedricamente isomorfi è che abbiano eguali invarianti.*

Il teorema si dimostra con tutta facilità. Siano infatti G, Γ due gruppi Abeliani oloedricamente isomorfi e siano $n_1, n_2, \ldots n_r$ gli invarianti del primo gruppo e

$$[g_1, g_2, \ldots g_r]$$

la base corrispondente. Indicando con $\gamma_1, \gamma_2, \ldots \gamma_r$ le corrispondenti sostituzioni di Γ, si vede subito che, a causa dell'isomorfismo oloedrico dei due gruppi,

$$[\gamma_1\, \gamma_2 \ldots \gamma_r]$$

è una base del secondo gruppo coi medesimi invarianti.

Viceversa, se G, Γ hanno eguali invarianti, ed hanno le rispettive basi

$$[g_1, g_2, \ldots g_r]$$
$$[\gamma_1, \gamma_2, \ldots \gamma_r],$$

basta far corrispondere a ciascuna g la γ col medesimo indice per stabilire una corrispondenza d'isomorfismo oloedrico fra i due gruppi.

Riesce ora molto naturale la domanda: *Dati ad arbitrio r numeri*

$$n_1, n_2 \ldots n_r,$$

di cui ciascuno sia divisore del precedente, esiste un gruppo Abeliano che li abbia per invarianti?

Si risponde subito affermativamente alla questione costruendo un gruppo di sostituzioni sopra $n_1 + n_2 + \ldots + n_r$ lettere

$$a_1 a_2 \ldots a_{n_1};\ b_1 b_2 \ldots b_{n_2};\ \ldots l_1 l_2 \ldots l_{n_r}$$

mediante le sostituzioni generatrici

$$g_1 = (a_1 a_2 \ldots a_{n_1}),\ g_2 = (b_1 b_2 \ldots b_{n_2}), \qquad g_r = (l_1 l_2 \ldots l_{n_r}).$$

Il gruppo

$$G = [g_1, g_2, \ldots g_r]$$

avrà appunto gli invarianti richiesti.

§. 35. — Un'altra classe importante di gruppi è quella dei *gruppi transitivi risolubili* sopra un numero primo p di lettere, della quale ci andiamo ora ad occupare.

Sia G un tale gruppo e sia

$$(4) \qquad G, G_1, G_2, \ldots G_{n-1}, 1$$

una sua serie di composizione, i fattori di composizione essendo, per ipotesi, numeri primi. Dimostriamo in primo luogo che *tutti i gruppi della serie, tranne l'identità, sono transitivi sulle p lettere.*

Il primo gruppo G della serie essendo transitivo, basterà mostrare che ad un gruppo G_{i-1} supposto transitivo, succede un gruppo G_i egualmente transitivo, se non è $G_i = 1$. Supponiamo al contrario G_{i-1} transitivo, G_i intransitivo e sia

$$a_1 a_2 \ldots a_\mu$$

uno dei sistemi di transitività in cui si scindono le p lettere rispetto

alle sostituzioni di G_i (§. 9). Se con b_1 indichiamo un'altra qualunque fra le p lettere, esisterà nel gruppo transitivo G_{i-1} una sostituzione U che porta a_1 in b_1 e, come il gruppo G_i unisce transitivamente $a_1, a_2, \ldots a_\mu$, così il gruppo $U^{-1} G_i U$ unirà transitivamente le lettere che U sostituisce a queste. Ma poichè $U^{-1} G_i U = G_i$, ne concludiamo che il sistema di transitività cui appartiene b_1 ha almeno μ lettere e, siccome vale la medesima considerazione invertendo a_1 con b_1, si vede che tutti i sistemi di transitività contengono un egual numero μ di lettere. Dunque μ dividendo p, avremo $\mu = 1$ ovvero $\mu = p$. Nel primo caso G_i si riduce all'identità, nel secondo esso è transitivo come si era asserito.

Segue da queste considerazioni che il penultimo gruppo G_{n-1}, dovendo essere transitivo, ha un ordine divisibile per p e d'altra parte il suo ordine, come fattore di composizione, deve essere un numero primo, onde sarà precisamente $= p$. Esso consterà dunque delle p potenze di una sostituzione ciclica S sulle p lettere e sarà dunque un gruppo ciclico

$$G_{n-1} = \Gamma = (1, S, S^2, \ldots S^{p-1}).$$

Dimostriamo ora che Γ sarà invariante non solo nel precedente G_{n-2}, ma in tutti gli altri ed in G stesso. Supponiamo per ciò d'avere constatato che Γ è invariante in G_i e dimostriamo che tale sarà anche in G_{i-1}. Siccome l'ordine di G_i è un divisore di $1 . 2 . 3 \ldots p$, contiene p soltanto alla prima potenza e, pel teorema di Sylow, G_i contenendo Γ come sottogruppo invariante, non ammette alcun altro sottogruppo d'ordine p. Ora se U è una sostituzione qualunque di G_i^{-1} si ha

$$U^{-1} G_i U = G_i$$

e per ciò $U^{-1} \Gamma U$ trovasi in G_i e coincide con Γ stesso. Dunque Γ è invariante anche in G_{i-1} c. d. d.

Per trovare dunque tutti i gruppi transitivi risolubili sopra un numero primo p di elementi, dobbiamo ricercare i gruppi sulle p lettere che contengono il gruppo ciclico Γ come sottogruppo invariante; basterà dunque trovare il più ampio di tali gruppi e in esso ed in tutti i suoi sottogruppi transitivi avremo i gruppi richiesti.

§. 36. — Il più ampio gruppo nel quale il gruppo ciclico

$$\Gamma = (1, S, S^2, \ldots S^{p-1})$$

è contenuto come sottogruppo invariante dicesi il *gruppo metaciclico*. Si

tratta di trovare tutte le sostituzioni di questo gruppo e in particolare determinarne l'ordine. Indichiamo le p lettere con

$$x_0\, x_1\, x_2 \ldots x_{p-1}\,,$$

distinguendole con indici presi rispetto al modulo p, talchè considereremo anche indici interi m qualunque colla convenzione che si prenda $x_m = x_r$, essendo r il minimo resto positivo di m (mod p). Potremo porre evidentemente, distribuendo convenientemente gl' indici:

$$S = (x_0\, x_1\, x_2 \ldots x_{p-1}).$$

Ogni sostituzione U del gruppo metaciclico deve trasformare S in una sua potenza S^r, talchè si abbia

$$U^{-1}\, S\, U = S^r.$$

Qualunque sia l'esponente r, purchè non divisibile per p, S^r è simile ad S e però esistono corrispondenti sostituzioni U. D'altronde S^r può scriversi in p modi diversi soltanto, quindi per ogni valore dato ad r nella serie

$$1,\ 2,\ 3 \ldots p - 1$$

abbiamo p sostituzioni U fra loro differenti. Del resto si vede subito che, se una delle sostituzioni richieste è U, le altre $p-1$ sono

$$S\,U,\ S^2U,\ \ldots S^{p-1}U.$$

Ne concludiamo intanto:

Il gruppo metaciclico è dell' ordine $p\,(p-1)$.

Se scriviamo S^r in un determinato modo, facendo cominciare il suo ciclo con x_0, come S, è chiaro che le $p-1$ sostituzioni corrispondenti

$$U_1 = 1\,,\ U_2\,,\ U_3 \ldots U_{p-1}$$

lasceranno ferma x_0 e le sostituzioni del gruppo metaciclico $G_{p\,(p-1)}$ si ripartiranno nel quadro:

$$\left\{\begin{array}{llll}
1 & ,\, S & ,\, S^2 & \ldots S^{p-1} \\
U_2 & ,\, S\,U_2 & ,\, S^2\,U_2 & \ldots S^{p-1}\,U_2 \\
U_3 & ,\, S\,U_3 & ,\, S^2\,U_3\,, & \ldots S^{p-1}\,U_3 \\
\ldots & \ldots & \ldots & \ldots \\
U_{p-1} & ,\, S\,U_{p-1} & S^2\,U_{p-1} & \ldots S^{p-1}\,U_{p-1}\,.
\end{array}\right.$$

53039

Fra queste soltanto quelle della prima verticale lasciano ferma x_0 e però formano, entro $G_{p\,(p-1)}$, un sottogruppo d'ordine $p-1$. È facile vedere che questo sottogruppo è ciclico, cioè è formato dalle potenze di una sostituzione ciclica sulle $p-1$ lettere

$$x_1\, x_2 \ldots x_{p-1}\,.$$

Se indichiamo infatti con g una radice primitiva (mod p), quella sostituzione U_g che trasforma

$$S = (x_0\, x_1\, x_2 \ldots x_{p-1})$$

in

$$S^g = (x_0\, x_g\, x_{2g} \ldots x_{(p-1)g})$$

avrà l'espressione

$$T = \begin{pmatrix} x_0 & x_g & x_{2g} & \ldots & x_{(p-1)g} \\ x_0 & x_1 & x_2 & \ldots & x_{p-1} \end{pmatrix}$$

e, decomposta in cicli, darà il solo ciclo

$$T = (x_1\, x_g\, x_{g^2} \ldots x_{g^{p-2}}).$$

Ne concludiamo: *Tutto il gruppo metaciclico si genera colle due sostituzioni elementari*

$$S = (x_0\, x_1\, x_2 \ldots x_{p-1})\,,\quad T = (x_1\, x_g\, x_{g^2} \ldots x_{g^{p-2}})\,;$$

le sue $p\,(p-1)$ sostituzioni sono date dalla formola

$$U = S^\beta\, T^\alpha \begin{cases} \alpha = 0,\, 1,\, 2 \ldots p-2 \\ \beta = 0,\, 1,\, 2 \ldots p-1\,. \end{cases}$$

Per vedere in quale sua potenza la S viene trasformata dalla $U = S^\beta\, T^\alpha$, basta vedere l'effetto di T^α. Ora, siccome la T moltiplica gli indici per g, la T^α li moltiplica per g^α, e si ha quindi

$$T^{-\alpha}\,(x_0\, x_1 \ldots x_{p-1})\, T^\alpha = (x_0\, x_{g^\alpha}\, x_{2g^\alpha} \ldots x_{(p-1)g^\alpha}) = S^{g^\alpha}.$$

Ne segue la formola generale

$$T^{-\alpha}\, S^\beta\, T^\alpha = S^{\beta\, g^\alpha} = S^{\beta_1},$$

dove

$$\beta_1 \equiv \beta\, g^\alpha \pmod{p}\,;$$

si ha dunque

$$S^\beta\ T^\alpha = T^\alpha\ S^{\beta_1}$$

$$\beta_1 \equiv \beta g^\alpha \pmod p\,,$$

e il gruppo metaciclico è quindi dato anche dalle $p\ (p-1)$ sostituzioni

$$T^\alpha\ S^\beta \begin{cases} \alpha = 0\,,\ 1\,,\ 2 \ldots p-2 \\ \beta = 0\,,\ 1\,,\ 2 \ldots p-1\,. \end{cases}$$

§. 37 — L'effetto di una sostituzione

$$S^\beta\ T^\alpha$$

del gruppo metaciclico è di portare ogni indice ν nell'indice

$$\nu' \equiv g^\alpha\ \nu + \beta g^\alpha \pmod p.$$

Se poniamo

$$g^\alpha = a\,,\ \beta g^\alpha = b\,,$$

il primo numero a percorrerà un sistema completo di resti (mod p) *escluso lo zero,* ed il secondo b un intero sistema completo. Possiamo dunque rappresentare analiticamente il gruppo metaciclico colla formola

$$(5) \qquad \nu' \equiv a\nu + b \pmod p \begin{cases} a = \quad 1\,,\ 2\,, \ldots p-1 \\ b = 0\,,\ 1\,,\ 2\,, \ldots p-1\,; \end{cases}$$

il gruppo ciclico Γ_p corrisponderà evidentemente alle sostituzioni con $a = 1$.

Come già abbiamo visto al §. 35, soltanto le sostituzioni di Γ_p, fra quelle di $G_{p(p-1)}$, hanno dunque un periodo p; le altre hanno un periodo divisore di $p-1$. Confermiamo direttamente questo risultato e troviamo l'effettivo periodo di ogni altra sostituzione del gruppo metaciclico osservando che, se U è la sostituzione (5), le sue potenze successive sono

$$U^2)\ \nu' \equiv a^2\,\nu + (a+1)\,b$$

$$U^3)\ \nu' \equiv a^3\,\nu + (a^2 + a + 1)\,b$$

$$\cdots\cdots\cdots\cdots$$

$$U^r)\ \nu' \equiv a^r\,\nu + (a^{r-1} + a^{r-2} + \ldots a + 1)\,b$$

Perchè risulti $U^r = 1$ occorre dunque che sia $a^r \equiv 1 \pmod p$; ma tale condizione è anche sufficiente perchè da

$$a^r - 1 = (a-1)\,(a^{r-1} + a^{r-2} + \ldots + a + 1) \equiv 0 \pmod p\,,$$

essendo $a \not\equiv 1 \pmod{p}$, segue anche

$$a^{r-1} + a^{r-2} + \ldots + a + 1 \equiv 0 \pmod{p}.$$

Dunque: *Le sostituzioni* (5) *del gruppo metaciclico con* $a \not\equiv 1 \pmod{p}$ *hanno per periodo l'esponente* r *cui appartiene* $a \pmod{p}$, *quelle con* $a \equiv 1$ *hanno per periodo* p.

Osserviamo che: *Il gruppo metaciclico è doppiamente transitivo.* E infatti, se i, k sono due indici qualunque, la sostituzione

$$\nu' \equiv (k - i)\nu + i \pmod{p}$$

porta gli indici 0, 1 in i, k rispettivamente. Come si vede, l'ordine $p(p-1)$ del gruppo metaciclico è il minimo compatibile col suo doppio grado di transitività. Delle due sostituzioni generatrici S, T del gruppo metaciclico la prima è pari, la seconda dispari e quindi fra le sostituzioni $S^\beta T^\alpha$ di $G_{p(p-1)}$ sono pari quelle con α pari e dispari le altre. Nella rappresentazione analitica (5) sono pari quelle in cui a è *residuo quadratico* $\pmod{p}$, impari quelle in cui a è *non residuo.* Le pari formano un sottogruppo invariante d'indice 2, che dicesi il *gruppo semimetaciclico.*

§. 38. — Servendosi dell'espressione analitica (5) delle sostituzioni del gruppo metaciclico, è facile determinare tutti i suoi sottogruppi. Per brevità di linguaggio diamo al coefficiente a nella (5) il nome di *moltiplicatore* della sostituzione e supponiamo che nelle sostituzioni di un sottogruppo G_1 di $G_{p(p-1)}$ si presentino tutti e soli i moltiplicatori

$$(6) \qquad a_1, \; a_2, \ldots a_r.$$

Poichè il moltiplicatore di una sostituzione composta è il prodotto dei moltiplicatori delle sostituzioni componenti, gli r numeri (6) debbono essere tali che, moltiplicati per uno qualunque di essi a_i, si riproducano, salvo l'ordine, rispetto al modulo p. A ciascun moltiplicatore a_i della serie (6) corrisponderà così una sostituzione sugli r numeri (6) e il complesso di queste sostituzioni formerà evidentemente un gruppo Abeliano d'ordine r. È facile vedere che questo gruppo è un gruppo ciclico.

E infatti, se a_i è un moltiplicatore qualunque in (6) e δ è il periodo della sostituzione corrispondente, si avrà

$$a_i^\delta \equiv 1 \pmod{p},$$

e siccome δ è un divisore di r, gli r numeri (6) saranno tutte radici dell'equazione

$$x^{\delta} \equiv 1 \pmod{p}. \tag{7}$$

Quindi, la congruenza binomia (7) avendo tante radici quante unità sono nel suo grado, sarà r in ogni caso un divisore di $p-1$ [1]) e, poichè la congruenza (7) ha precisamente r radici, si conclude che esse saranno tutti e soli i moltiplicatori (6). Dunque: *I moltiplicatori distinti delle sostituzioni di un sottogruppo del gruppo metaciclico sono tutte e sole le r radici di una congruenza binomia $x^r \equiv 1 \pmod{p}$, essendo r un divisore di $p-1$.*

È ben noto che fra le radici della (7) vi sono di quelle che appartengono precisamente all'esponente r e il loro numero è $\varphi(r)$ [2]), onde risulta la proprietà sopra enunciata: *Il gruppo dei moltiplicatori è un gruppo ciclico.*

Tornando al sottogruppo G_1 supposto di G, distinguiamo due casi secondo che in G_1 trovansi più sostituzioni con un dato moltiplicatore a ovvero una sola.

Se si hanno in G_1 due sostituzioni distinte

$$U = \begin{pmatrix} a\nu + b \\ \nu \end{pmatrix}, \quad U_1 = \begin{pmatrix} a\nu + b_1 \\ \nu \end{pmatrix}$$

col medesimo moltiplicatore a, avremo in G_1 anche la sostituzione inversa di U:

$$U^{-1} = \begin{pmatrix} a^{-1}(\nu - b) \\ \nu \end{pmatrix} \text{ [3])},$$

quindi anche

$$V = U^{-1} U_1 = \begin{pmatrix} \nu + b_1 - b \\ \nu \end{pmatrix}.$$

---

[1]) Dirichlet, *Zahlentheorie*, §. 31.

[2]) Gauss, *Disquisitiones arithmeticae*, art. 54. — Dirichlet, *Zahlentheorie*, §. 29.

[3]) Con a^{-1} indichiamo il numero intero a_1 che soddisfa la congruenza $a\,a_1 \equiv 1 \pmod{p}$.

Essendo $b_1 - b \not\equiv 0 \pmod{p}$, le potenze di V danno in G_1 il gruppo ciclico Γ_p; quindi per ogni moltiplicatore a_i sono contenute in G_1 tutte le sostituzioni

$$\nu' \equiv a_i \nu + b \quad \{ b = 0, 1, 2 \ldots p - 1.$$

Ne segue che, se per un *dato* moltiplicatore a si ha in G_1 una sola sostituzione, per ogni altro moltiplicatore si avrà egualmente una sola sostituzione. Se scegliamo dunque fra i moltiplicatori (6) uno che appartenga all'esponente r, ed è

$$\nu' \equiv a\nu + b \pmod{p}$$

la sostituzione corrispondente, le r potenze di questa sostituzione esauriranno tutto il sottogruppo G. È chiaro che le sostituzioni di un tale sottogruppo lasciano tutte ferma una medesima lettera ed ogni sottogruppo di questa specie è perfettamente determinato dal suo ordine e dalla lettera che lascia ferma. Nel caso contrario, G_1 consterà delle $p\,r$ sostituzioni della forma

$$\nu' \equiv a_i \nu + b \pmod{p}, \tag{8}$$

percorrendo b un sistema completo di resti (mod p) e a_i le r radici (6) della congruenza $x^r \equiv 1 \pmod{p}$. Concludiamo dunque:

Il gruppo metaciclico contiene soltanto i seguenti sottogruppi:

a) sottogruppi ciclici d'ordine r divisore di $p-1$, generati dalle potenze di una sostituzione a periodo r.

b) sottogruppi (8) *dell'ordine $p\,r$, ove b percorre un sistema completo di resti* (mod p) *e a_i le radici della congruenza $x^r \equiv 1$* (mod p).

Anche qui per il gruppo metaciclico, come per i gruppi Abeliani (§. 30), vediamo che esistono sottogruppi di tutti gli ordini divisori dell'ordine del gruppo. Ma il risultato, nel caso attuale, è ancora più completo in quanto che conosciamo effettivamente tutti i possibili sottogruppi. Fra questi i più interessanti sono i sottogruppi (8) d'ordine $p\,r$, che ci risolvono il problema, da cui siamo partiti al §. 34, di trovare cioè tutti i gruppi transitivi risolubili sopra un numero primo p di elementi. Siccome, per ogni divisore r di $p-1$, esiste un solo sottogruppo dell'ordine pr, vediamo che: *Ogni sottogruppo d'ordine $p\,r$ del gruppo metaciclico è un suo sottogruppo invariante.* Ciò si vede del resto anche subito

dalla forma (8) delle sostituzioni del sottogruppo. Se scindiamo $p-1$ nei suoi fattori primi

$$p_1 , p_2 , \ldots p_r$$

diversi od eguali, avremo la serie di composizione

$$G_{p(p-1)} , G_{\frac{p(p-1)}{p_1}} , G_{\frac{p(p-1)}{p_1 p_2}} \ldots \Gamma_p 1 .$$

Ne risulta il teorema: *Il gruppo metaciclico è un gruppo risolubile; i suoi fattori di composizione sono i fattori primi di $p-1$ e il numero p.*

Come i gruppi Abeliani, così anche il gruppo metaciclico offre la particolarità che ogni sua serie di composizione è una serie principale.

§. 39 — Un'altra interessante classe di gruppi si ottiene considerando, invece che sostituzioni lineari intere (5) sugli indici, delle sostituzioni ancora lineari ma frazionarie. Questi gruppi, che hanno un'importanza grandissima nella teoria della trasformazione delle funzioni ellittiche e delle equazioni modulari, ci offriranno qui, nel campo elementare, notevoli esempii di gruppi semplici.

Essendo ancora p un numero primo, consideriamo $p+1$ lettere

$$x_\infty , x_0 , x_1 , x_2 , \ldots x_{p-1}$$

contraddistinte dai $p+1$ indici

$$(a) \qquad \infty , 0 , 1 , 2 , \ldots p-1 ,$$

e la formola

$$\text{(I)} \qquad \nu' \equiv \frac{\alpha \nu + \beta}{\gamma \nu + \delta} \text{ [1]} \pmod{p} ,$$

---

[1]) Ricordiamo che nella teoria dei numeri col simbolo frazionario $\frac{a}{b}$ (mod p) si intende quel numero *intero* x che soddisfa la congruenza $b x \equiv a$ (mod p), che esiste ed è unico se $b \not\equiv 0$ (mod p). Quando sia $b \equiv 0$ (mod p), ma naturalmente $a \not\equiv 0$, s'intenderà per $\frac{a}{b}$ il valore ∞. Queste frazioni, come si rileva da considerazioni elementari sulle congruenze, obbediscono alle medesime leggi delle ordinarie; di queste proprietà ci serviamo ripetutamente nel testo.

dove $\alpha, \beta, \gamma, \delta$ sono numeri interi qualunque, tali però che sia

$$\alpha\delta - \beta\gamma \not\equiv 0 \pmod{p},$$

dà una effettiva sostituzione sui $p+1$ indici (a), perchè la (I) trasporta allora, come subito si vede, indici diversi in indici diversi. Si noti che i numeri $\alpha, \beta, \gamma, \delta$ nella (I) sono presi non in modo assoluto, ma soltanto rispetto al modulo p. La (I) non rimane alterata scrivendola

$$(\mathrm{I}^*) \qquad \nu' \equiv \frac{r\alpha\nu + r\beta}{r\gamma\nu + r\delta} \pmod{p},$$

con r intero qualunque, purchè sia $r \not\equiv 0 \pmod{p}$. Viceversa due sostituzioni (I) sono identiche allora soltanto quando i coefficienti $\alpha, \beta, \gamma, \delta$ dell'una siano proporzionali (mod p) a quelli dell'altra. Il *determinante* $\Delta = \alpha\delta - \beta\gamma$ della (I) si cangia nella (I*) in $r^2\Delta$ e rimane quindi residuo o non residuo quadratico (mod p) a seconda del carattere di Δ. Se Δ è residuo, se cioè, col simbolo di Legendre, $\left(\frac{\Delta}{p}\right) = +1$ potremo rendere

$$r^2\Delta \equiv 1 \pmod{p}$$

e se Δ è non residuo, cioè $\left(\frac{\Delta}{p}\right) = -1$, potremo fare

$$r^2\Delta \equiv q \pmod{p},$$

essendo q un non residuo fisso.

La totalità delle sostituzioni (I) è quindi identica a quella che si ottiene facendo percorrere ad $\alpha, \beta, \gamma, \delta$ tutti i numeri che soddisfano alla congruenza

$$(9) \qquad \alpha\delta - \beta\gamma \equiv 1 \pmod{p},$$

o all'altra

$$(9^*) \qquad \alpha\delta - \beta\gamma \equiv q \pmod{p}.$$

Due sostituzioni (I), che soddisfino alla (9) o alla (9*), saranno identiche soltanto quando i nuovi valori $\alpha', \beta', \gamma', \delta'$ di $\alpha, \beta, \gamma, \delta$ soddisfino le congruenze

$$\alpha' \equiv \pm\alpha, \ \beta' \equiv \pm\beta, \ \gamma' \equiv \pm\gamma, \ \delta' \equiv \pm\delta \pmod{p}.$$

Tutte le sostituzioni (I) formano un gruppo poichè, se si ha:

$$\nu' \equiv \frac{\alpha\,\nu + \beta}{\gamma\,\nu + \delta}\,,\quad \nu'' \equiv \frac{\alpha'\nu' + \beta'}{\gamma'\nu' + \delta'} \pmod{p}\,,$$

ne segue

$$\nu'' \equiv \frac{(\alpha'\,\alpha + \beta'\,\gamma)\,\nu + (\alpha'\,\beta + \beta'\,\delta)}{(\gamma'\,\alpha + \delta'\,\gamma)\,\nu + (\gamma'\,\beta + \delta'\,\delta)} \pmod{p}.$$

Indicando simbolicamente la sostituzione (I) con

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix},$$

si vede che due sostituzioni (I) si compongono in una sostituzione della medesima specie secondo la formola

$$\text{(II)} \qquad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\,\alpha' + \gamma\,\beta', & \beta\,\alpha' + \delta\,\beta' \\ \alpha\,\gamma' + \gamma\,\delta', & \beta\,\gamma' + \delta\,\delta' \end{pmatrix},$$

onde si vede che: *il determinante della sostituzione composta è eguale al prodotto dei determinanti delle componenti.*

Il gruppo delle sostituzioni (I) sui $p+1$ indici (a) si dirà il *gruppo lineare totale.* Si tratta in primo luogo di valutarne l'ordine, per il che basta contare quante soluzioni distinte, e non opposte in segno, hanno le congruenze (9) (9*).

Ora si osservi che, nella (9) p. e., se

$$\gamma \equiv 0 \pmod{p}\,,$$

possiamo dare a β qualunque valore, ad α qualunque valore, escluso $\alpha \equiv 0$, (mod p) e dal valore di α risulta individuato quello di δ; dunque la (9) ha

$$p\,(p-1) \text{ soluzioni con } \gamma \equiv 0 \pmod{p}.$$

Se poi $\gamma \not\equiv 0$ (mod p), si può dare sì ad α che a δ valori arbitrarii e fissati α, δ è fissato anche β, onde la (9) ha:

$$p^2\,(p-1) \text{ sostituzioni con } \gamma \not\equiv 0 \pmod{p}.$$

Il numero totale delle soluzioni della (9) è dunque

$$p\,(p-1) + p^2\,(p-1) = p\,(p-1)\,(p+1)$$

e lo stesso vale evidentemente della (9*).

Ma poichè due soluzioni opposte danno la medesima sostituzione (I), abbiamo il risultato:

Il gruppo lineare totale (I) *contiene*

$$p\,(p^2-1)$$

sostituzioni. Lo indicheremo per ciò con $G_{p\,(p^2-1)}$. In questo gruppo le sostituzioni che soddisfano alla congruenza (9) formano evidentemente un sottogruppo invariante d'indice 2.

Questo gruppo $G_{\frac{p(p^2-1)}{2}}$, *definito dalla formola*

$$\text{(III)} \qquad \nu' \equiv \frac{\alpha\,\nu+\beta}{\gamma\,\nu+\delta}, \quad \alpha\,\delta-\beta\,\gamma \equiv 1 \pmod{p},$$

si dirà il gruppo lineare speciale od anche il gruppo modulare [1]).

Osserviamo ora che: *il gruppo lineare totale è triplamente transitivo sulle* $p+1$ *lettere*. E infatti, se i, k, l sono tre indici qualunque diversi, la sostituzione

$$\nu' \equiv \frac{l-i}{l-k}\cdot\frac{\nu-k}{\nu-i}$$

trasporta rispettivamente gli indici i, k, l in ∞, 0, 1. Come il gruppo metaciclico, anche il gruppo lineare, ha il minimo ordine compatibile col suo grado triplo di transitività.

§. 40. — Per determinare i diversi periodi che possono offrire le sostituzioni (I) del gruppo lineare, cominciamo dal ricercare se vi sono indici che rimangono fissi per una sostituzione (I).

Se x è un tale indice, dovremo avere

$$x \equiv \frac{\alpha\,x+\beta}{\gamma\,x+\delta} \pmod{p}$$

cioè

$$\gamma\,x^2+(\delta-\alpha)\,x-\beta \equiv 0 \pmod{p}.$$

Escludendo per un momento il caso $\gamma \equiv 0$, che dà le note sostituzioni del gruppo metaciclico, la precedente congruenza, moltiplicata per $4\,\gamma$, diventa

$$\text{(10)} \qquad \{2\,\gamma\,x+\delta-\alpha\}^2 \equiv D \pmod{p},$$

---

[1]) Quest'ultima denominazione proviene dalla teoria delle equazioni modulari per le funzioni ellittiche.

ove si è posto

$$D \equiv (\delta - \alpha)^2 + 4\beta\gamma = (\alpha + \delta)^2 - 4\Delta. \tag{11}$$

Ed ora distinguiamo tre casi:

a) Sia $D \equiv 0 \pmod{p}$. Allora la (10) ha una sola radice e però la sostituzione lascia ferma una lettera, spostando tutte le altre. La sostituzione dicesi *parabolica*.

b) Sia $D \not\equiv 0 \pmod{p}$ e D residuo quadratico di p, ossia $\left(\frac{D}{p}\right) = +1$. La (10) ha allora due radici distinte e la sostituzione, che lascia ferme due lettere spostando le rimanenti $p-1$, dicesi *ellittica*.

c) Sia $D \not\equiv 0$ non residuo (mod p), cioè

$$\left(\frac{D}{p}\right) = -1.$$

La (10) non ha allora radici e la sostituzione, che sposta tutte le $p+1$ lettere, dicesi *iperbolica*.

Nel caso escluso $\gamma \equiv 0 \pmod{p}$ la (I) appartiene al gruppo metaciclico e lascia fisso l'indice ∞ e nessun altro indice se $\alpha \equiv \delta \pmod{p}$ cioè se $D \equiv 0 \pmod{p}$, invece un secondo indice se $\alpha - \delta \not\equiv 0$, nel qual caso $\left(\frac{D}{p}\right) = +1$. La sostituzione è parabolica nel primo caso, ellittica nel secondo, onde vediamo che il caso $\gamma \equiv 0$ rientra nel caso generale. Determiniamo ora successivamente il periodo delle tre diverse specie di sostituzioni in $G_{p(p^2-1)}$ osservando che due sostituzioni *affini* nel gruppo (§. 25) appartengono evidentemente alla medesima specie.

a) Sostituzioni paraboliche.* Se la sostituzione S in discorso lascia ferma x_i, prendiamo in G una sostituzione T che porti x_i in x_∞ e la sostituzione $T^{-1}ST$ sarà evidentemente una sostituzione parabolica che lascia ferma x_∞ ed avrà quindi la forma

$$\nu' \equiv \nu + b.$$

E poichè S e $T^{-1}ST$ hanno il medesimo periodo ne concludiamo:

Le sostituzioni paraboliche hanno il periodo p.

b) Sostituzioni ellittiche.* La S lasci fermi i due indici x_i, x_k e sia T una sostituzione di $G_{p(p^2-1)}$ che porti x_i, x_k in x_0, x_∞; la $T^{-1}ST$ avrà la forma

$$\nu' \equiv a\nu \pmod{p}$$

ed avrà per periodo quel divisore di $p-1$ cui appartiene a. Dunque: *Le sostituzioni ellittiche hanno un periodo divisore di* $p-1$.

c^*) *Sostituzioni iperboliche.* Una sostituzione iperbolica sposta tutte le $p+1$ lettere e noi dimostriamo che, ove si decomponga in cicli, conterrà in ogni ciclo il medesimo numero di lettere, onde seguirà subito il teorema: *Le sostituzioni iperboliche hanno un periodo divisore di* $p+1$.

Decomponendo la S iperbolica in cicli si abbia

$$S = C_1 C_2 C_3 \ldots$$

Se l'ordine r di C_1 fosse minore dell'ordine s di C_2 la S^r, senza essere l'identità, lascierebbe ferme r lettere, ciò che è impossibile se non è $r=2$. Ma allora la S contiene un ciclo di 2.° ordine ed è affine ad una sostituzione (iperbolica) S_1 che contiene il ciclo $(0\ \infty)$; questa S_1, avendo l'espressione analitica

$$\nu' \equiv \frac{b}{\nu} \pmod{p},$$

è a periodo 2, quindi anche la S, e tutti i cicli di S sono di 2.° ordine c. d. d.

§. 41. — Si è già visto come nel gruppo lineare totale sia contenuto, quale sottogruppo invariante d'indice 2, il gruppo modulare (III):

$$\text{(III)} \qquad \nu' \equiv \frac{\alpha\nu+\beta}{\gamma\nu+\delta}, \quad \alpha\delta-\beta\gamma \equiv 1 \pmod{p}.$$

Si noti che il *gruppo modulare è doppiamente transitivo.* E infatti la sostituzione

$$\nu' \equiv \frac{k\nu+(kl-1)}{\nu+l}$$

di questo gruppo porta gli indici ∞, 0 in $k, k-l^{-1}$, che sono due indici qualunque.

Per prepararci a dimostrare, come faremo nel prossimo §., che il gruppo modulare, appena $p>3$, è semplice, è utile osservare che *l'intero gruppo modulare si può generare mediante le due sostituzioni elementari*

$$S = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix},$$

ossia

$$\mathrm{S})\ \nu' \equiv \nu + 1\ ,\ \ \mathrm{T})\ \nu' \equiv -\frac{1}{\nu} \pmod{p}.$$

Cominciamo per ciò dall'osservare che con S, T si compone la sostituzione

$$\mathrm{S}_1 = \mathrm{T}\,\mathrm{S}^{-1}\,\mathrm{T} = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}.$$

Nel gruppo Γ generato da S, T esiste dunque qualunque potenza di S o di S_1 indi

$$\mathrm{S}^b = \begin{pmatrix} 1, & b \\ 0, & 1 \end{pmatrix} \quad \mathrm{S}_1{}^c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

e però

$$\mathrm{S}^b\,\mathrm{S}_1{}^c = \begin{pmatrix} 1, & b \\ c, & 1 + b\,c \end{pmatrix}$$

con b, c qualunque. Preso c in guisa che sia $b\,c \equiv -1 \pmod{p}$, avremo dunque in Γ

$$\begin{pmatrix} 1 & , b \\ -b^{-1}, & 0 \end{pmatrix}$$

con b qualunque $\not\equiv 0 \pmod{p}$, come anche

$$\begin{pmatrix} 0 & , b \\ -b^{-1}, & 0 \end{pmatrix} \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix} = \begin{pmatrix} b^{-1}, & 0 \\ 0 & , b \end{pmatrix}.$$

Ora prendiamo una qualunque sostituzione $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ del gruppo modulare; se è $\alpha \equiv 0 \pmod{p}$ si ha

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} 0 & , \beta \\ -\beta^{-1} & , \delta \end{pmatrix};$$

ma

$$\begin{pmatrix} 0 & , \beta \\ -\beta^{-1} & , \delta \end{pmatrix} = \begin{pmatrix} 1, & -\beta\,\delta \\ 0, & 1 \end{pmatrix} \begin{pmatrix} 0 & , \beta \\ -\beta^{-1} & , 0 \end{pmatrix}$$

e le componenti a destra sono in Γ, quindi anche $\begin{pmatrix} 0 & , \beta \\ -\beta^{-1} & , \delta \end{pmatrix}$. Similmente una sostituzione qualunque (III) con $\beta \equiv 0 \pmod{p}$ è data da

$$\begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix}$$

e siccome

$$\begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} 1 & , 0 \\ \alpha\gamma, & 1 \end{pmatrix} \begin{pmatrix} \alpha, & 0 \\ 0, & \alpha^{-1} \end{pmatrix}$$

e le due sostituzioni a destra sono in Γ, vi è anche $\begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix}$.

Siano ora $\alpha \not\equiv 0$, $\beta \not\equiv 0 \pmod{p}$. Siccome

$$\begin{pmatrix} 1, & m \\ 0, & 1 \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} \alpha, & \beta + m\alpha \\ \gamma, & \delta + m\gamma \end{pmatrix},$$

basta determinare m dalla congruenza

$$m\alpha + \beta \equiv 0 \pmod{p},$$

per avere a destra una sostituzione con $\beta \equiv 0 \pmod{p}$, quindi di Γ. Così il nostro teorema è dimostrato.

Delle due sostituzioni S, T generatrici del gruppo modulare la prima è parabolica e la seconda è ellittica, ovvero iperbolica secondo che $\left(\frac{-1}{p}\right) = +1$, ovvero $\left(\frac{-1}{p}\right) = -1$, cioè secondo che $p \equiv 1$, ovvero $p \equiv 3 \pmod{4}$. Si vede inoltre facilmente che S, T sono ambedue pari. Per la prima, che è a periodo p, ciò è evidente. Per la seconda basta osservare che, se $p \equiv 1 \pmod{4}$, essa è ellittica e si decompone in $\frac{p-1}{2}$ cicli di 2 lettere; se invece $p \equiv 3 \pmod{4}$, è iperbolica e consta di $\frac{p+1}{2}$ cicli di 2 lettere. Il gruppo modulare contiene adunque tutte sostituzioni pari, laddove il gruppo lineare totale ne contiene anche delle dispari, come la

$$\begin{pmatrix} g, & 0 \\ 0, & 1 \end{pmatrix},$$

essendo g radice primitiva (mod p). Come sostituzioni generatrici del gruppo lineare totale potremo quindi prendere le tre seguenti

$$S = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad U = \begin{pmatrix} g, & 0 \\ 0, & 1 \end{pmatrix},$$

§. 42. — Andiamo ora a dimostrare l'importante teorema:

Il gruppo modulare Γ *di* $\frac{p(p^2-1)}{2}$ *sostituzioni sopra* $p+1$ *lettere è semplice, appena* $p > 3$.

Per $p = 3$ il teorema non vale perchè il gruppo modulare non è allora altro che il gruppo alterno su 4 elementi.

Supponiamo che in Γ esista un sottogruppo invariante H. Essendo Γ doppiamente transitivo, sarà H almeno una volta transitivo; giacchè da una sostituzione di Γ

$$h = (x_i\, x_k \ldots) \ldots,$$

trasformata con una conveniente sostituzione di Γ, si può ottenere una nuova sostituzione

$$h' = (x_\infty\, x_l \ldots) \ldots$$

di H che trasporti la lettera x_∞ in un'altra qualunque x_l. L'ordine di H dovrà dunque essere divisibile per $p+1$. Ciò premesso, dimostriamo successivamente:

1.°) H *non può contenere sostituzioni paraboliche.*

Sia h una sostituzione parabolica di H che lasci ferma x_i; trasformandola con una γ di Γ che porti x_i in x_∞, otterremo in H la sostituzione parabolica

$$h_1 = \gamma^{-1} h \gamma$$

che lascierà ferma x_∞ ed avrà quindi la forma

$$h_1 = \begin{pmatrix} 1, & \beta \\ 0, & 1 \end{pmatrix} \quad (\beta \not\equiv 0 \pmod{p}).$$

Tutte le potenze di h_1 e in particolare

$$S = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix} = h_1^{\beta^{-1}}$$

saranno in H.

Ora H, essendo invariante in Γ, se contiene una sostituzione

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix},$$

contiene anche le trasformate per mezzo di T, S cioè

$$T \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} T = \begin{pmatrix} -\delta, & \gamma \\ \beta, & -\alpha \end{pmatrix}$$

$$S^{-1} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} S = \begin{pmatrix} \alpha+\gamma, & (\beta+\delta)-(\alpha+\gamma) \\ \gamma, & \delta-\gamma \end{pmatrix}.$$

Contenendo $\begin{pmatrix} 1, & \gamma \\ 0, & 1 \end{pmatrix}$ con γ qualunque, H contiene anche

$$T \begin{pmatrix} 1, & \gamma \\ 0, & 1 \end{pmatrix} T = \begin{pmatrix} 1 & 0 \\ -\gamma & 1 \end{pmatrix},$$

indi

$$\begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix} = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = T.$$

Dunque H, contenendo le sostituzioni elementari S, T, coincide con Γ c. d. d.

2.°) H *non può contenere sostituzioni ellittiche.*

Se H contiene una sostituzione ellittica ne conterrà anche, a causa della doppia transitività di Γ, una affine che lascerà fermi gli indici 0, ∞ ed avrà quindi la forma

$$h = \begin{pmatrix} \alpha, & 0 \\ 0, & \alpha^{-1} \end{pmatrix}.$$

In H si troverà anche

$$h_1 = S^{-1} h S = \begin{pmatrix} \alpha, & \alpha^{-1}-\alpha \\ 0, & \alpha^{-1} \end{pmatrix}$$

e per ciò anche

$$h_1 h^{-1} = \begin{pmatrix} 1, & \alpha^{-1}(\alpha^{-1}-\alpha) \\ 0, & 1 \end{pmatrix},$$

che è parabolica. Dunque H coincide con Γ.

3.°) Resta dunque soltanto da vedersi se con sostituzioni tutte iperboliche si può comporre un sottogruppo H invariante in Γ. L'ordine di H essendo divisibile per $p+1$ indi per 2, esiste in H una sostituzione (iperbolica) a periodo 2 e quindi una affine contenente il ciclo $(0\ \infty)$; questa avrà dunque la forma

$$h = \begin{pmatrix} 0 & , \beta \\ -\beta^{-1} & , 0 \end{pmatrix}$$

e, perchè h è iperbolica, dovrà essere

$$\left(\frac{-4}{p}\right) = \pm 1,$$

quindi intanto $p \equiv 3 \pmod 4$. In H avremmo altresì

$$h_1 = \mathrm{T}\, h\, \mathrm{T} = \begin{pmatrix} 0 & , -\beta^{-1} \\ \beta & , 0 \end{pmatrix}$$

e però

$$h h_1 = \begin{pmatrix} \beta^{-2} & , 0 \\ 0 & , \beta^2 \end{pmatrix},$$

la quale è ellittica se non è l'identità.

Dunque è $\beta^4 \equiv 1 \pmod p$ e per ciò, essendo $p \equiv 3 \pmod 4$, sarà $\beta \equiv \pm 1 \pmod p$, onde h coincide necessariamente con

$$\mathrm{T} = \begin{pmatrix} 0 & , 1 \\ -1 & , 0 \end{pmatrix}.$$

Insieme a T avremo in H qualunque sua trasformata

$$h' = \begin{pmatrix} \alpha & , \beta \\ \gamma & , \delta \end{pmatrix}^{-1} \begin{pmatrix} 0 & , 1 \\ -1 & , 0 \end{pmatrix} \begin{pmatrix} \alpha & , \beta \\ \gamma & , \delta \end{pmatrix} = \begin{pmatrix} -(\alpha\gamma+\beta\delta) & \alpha^2+\beta^2 \\ -(\gamma^2+\delta^2) & , \alpha\gamma+\beta\delta \end{pmatrix},$$

purchè sia

$$\alpha\delta - \beta\gamma \equiv 1 \pmod p.$$

Prendiamo

$$\gamma = \delta = 1 \begin{cases} \alpha - \beta \equiv 1 \\ \alpha + \beta \equiv 0 \end{cases}$$

cioè $2\alpha \equiv 1$, $2\beta \equiv -1$, indi $\alpha^2+\beta^2 \equiv 2^{-1}$ e sarà

$$h' = \begin{pmatrix} 0\,, & 2^{-1} \\ -2\,, & 0 \end{pmatrix}$$

sicchè, per quanto sopra si è visto, avremo

$$2 \equiv \pm 1 \pmod{p}\,,$$

onde necessariamente vale il segno inferiore e si ha $p=3$ c. d. d.

Si osservi che pei valori

$$p = 5\,,\ 7\,,\ 11$$

il gruppo *semplice* modulare è dei rispettivi ordini

$$60\,,\ 168\,,\ 660\,.$$

Il primo è oloedricamente isomorfo col gruppo alterno su 5 lettere (§. 29), gli altri due sono i tipi di gruppi semplici già citati al §. 28.

Terminiamo queste ricerche sul gruppo modulare col dimostrare il teorema seguente, che è importante nella teoria delle equazioni modulari:

Il più ampio gruppo di sostituzioni sui $p+1$ *indici* $\infty, 0, 1, 2, \ldots p-1$, *nel quale il gruppo modulare* Γ *sia contenuto come sottogruppo invariante, è il gruppo lineare* $G_{p(p^2-1)}$.

Sia U una sostituzione sui $p+1$ indici che trasformi Γ in se medesimo:

$$U^{-1}\,\Gamma\,U = \Gamma\,.$$

Combinando la U con una conveniente γ, si avrà una sostituzione equivalente

$$U_1 = \gamma\,U$$

che lascia fermo l'indice ∞, e sarà ancora

$$U_1^{-1}\,\Gamma\,U_1 = \Gamma.$$

Le sostituzioni di Γ che lasciano fisso l'indice ∞ sono quindi trasformate da U_1 in altrettali sostituzioni, cioè U_1 trasformerà il gruppo semi-metaciclico

$$\nu' \equiv a\,\nu + b \pmod{p} \qquad \left(\frac{a}{p}\right) = +1$$

in se medesimo e quindi la sostituzione $S = \begin{pmatrix} 1\,, & 1 \\ 0\,, & 1 \end{pmatrix}$ in una sua potenza.

Dunque la U_1 sarà nel gruppo metaciclico (§. 36) ed U apparterrà in conseguenza al gruppo lineare $G_{p(p^2-1)}$ c. d. d.

Per le medesime ragioni è chiaro che il gruppo lineare stesso non è contenuto come sottogruppo invariante in alcun gruppo più ampio.

Capitolo IV.

Gruppi finiti di sostituzioni lineari sopra una variabile. — Loro rappresentazione geometrica come gruppi dei poliedri regolari.

§. 43. — Una interessante applicazione della teoria generale dei gruppi si trova nella determinazione di tutti i gruppi possibili finiti di sostituzioni lineari sopra una variabile, che formerà l'oggetto del presente capitolo.

Consideriamo una variabile z, che assume tutti i valori reali e complessi e le sostituzioni lineari

$$(1) \qquad z' = \frac{\alpha z + \beta}{\gamma z + \delta},$$

dove i coefficienti α, β, γ, δ sono costanti qualunque complesse, colla condizione però che il determinante $\alpha\delta - \beta\gamma$ della sostituzione non sia zero, condizione necessaria affinchè la (1) rappresenti un'effettiva sostituzione [1]). Indicando simbolicamente la sostituzione (1) con $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, si vede subito che due sostituzioni $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, $\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}$, successivamente eseguite, si compongono nella terza (Cf. §. 39):

$$(a) \qquad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \gamma\beta', & \beta\alpha' + \delta\beta' \\ \alpha\gamma' + \gamma\delta', & \beta\gamma' + \delta\delta' \end{pmatrix}.$$

Le sostituzioni lineari (1) sono operazioni che soddisfano a tutte le leggi fondamentali enunciate al §. 15, che permettono di considerare gruppi finiti od infiniti di queste operazioni. Tanto si deduce subito

---

[1]) Se fosse $\alpha\delta - \beta\gamma = 0$, il 2.° membro della (1) sarebbe indipendente da z.

dalla legge (a) di composizione, ovvero *a priori* dal significato delle operazioni stesse [1]).

Ci proponiamo di costruire tutti i possibili gruppi *finiti* di sostituzioni lineari (1). Come esempio effettivo di tali gruppi citiamo quello, ben noto in geometria, dei 6 valori del rapporto anarmonico per quattro elementi di una forma geometrica di 1.ª specie. Detto z uno di questi valori, i 6 valori sono

$$z\,,\ 1-z,\ \frac{1}{z}\,,\ \frac{1}{1-z}\,,\ \frac{z}{z-1}\,,\ \frac{z-1}{z}$$

e queste 6 sostituzioni lineari formano evidentemente un gruppo [2]).

Cominciamo dall'osservare che se nella (1) si cangia linearmente la variabile z in

$$Z=\frac{a\,z+b}{c\,z+d}=z\begin{pmatrix}a\,,\ b\\ c\,,\ d\end{pmatrix}$$

e colla medesima sostituzione la variabile trasformata z' in

$$Z'=z'\begin{pmatrix}a\,,\ b\\ c\,,\ d\end{pmatrix},$$

sarà Z legata linearmente a Z' dalla sostituzione

$$Z'=Z.\begin{pmatrix}a\,,\ b\\ c\,,\ d\end{pmatrix}^{-1}\begin{pmatrix}\alpha\,,\ \beta\\ \gamma\,,\ \delta\end{pmatrix}\begin{pmatrix}a\,,\ b\\ c\,,\ d\end{pmatrix}.$$

Se consideriamo un insieme di sostituzioni (1) che formino un gruppo G, cangiando linearmente la variabile avremo il gruppo trasformato

$$G'=\begin{pmatrix}a\,,\ b\\ c\,,\ d\end{pmatrix}^{-1}G\begin{pmatrix}a\,,\ b\\ c\,,\ d\end{pmatrix},$$

che riguardiamo come appartenente al medesimo tipo di G. Il nostro problema sarà quindi quello di determinare tutti i tipi possibili di gruppi finiti di sostituzioni lineari.

---

[1]) Una sostituzione (1) può riguardarsi come un'ordinaria sostituzione; soltanto gli elementi che la sostituzione permuta fra loro invece di esser in numero finito sono in numero infinito, anzi formano la doppia infinità dei valori complessi di z.

[2]) Nella successiva classificazione (§. 45) questo apparirà come gruppo diedrale per $n=3$.

A fondamento della nostra ricerca poniamo le osservazioni seguenti. La sostituzione (1) lascia fissi due valori della variabile complessa z, cioè le radici della equazione

$$\gamma z^2 + (\delta - \alpha) z - \beta = 0 , \tag{2}$$

che possono essere distinti o coincidenti. Non fa eccezione il caso in cui, essendo $\gamma = 0$, la (2) si riduce al 1.° grado; allora uno dei poli è in $z = \infty$ e l'altro in $\frac{\beta}{\delta - \alpha}$ che è distinto dal primo se $\alpha \neq \delta$. È chiaro che se la sostituzione $\begin{pmatrix} \alpha , & \beta \\ \gamma , & \delta \end{pmatrix}$ ha i poli z_1, z_2 e la $\begin{pmatrix} a , & b \\ c , & d \end{pmatrix}$ trasporta z_1, z_2 in z'_1, z'_2, la trasformata

$$\begin{pmatrix} a , & b \\ c , & d \end{pmatrix}^{-1} \begin{pmatrix} \alpha , & \beta \\ \gamma , & \delta \end{pmatrix} \begin{pmatrix} a , & b \\ c , & d \end{pmatrix}$$

avrà i poli z'_1, z'_2. Ora dimostriamo il teorema:

Ogni sostituzione lineare (1), *che fa parte di un gruppo finito* G, *ha necessariamente i suoi due poli distinti.*

Basterà dimostrare la cosa per una conveniente sostituzione trasformata. Ora questa si può sempre scegliere in guisa che uno dei suoi poli sia in $z = \infty$ e, se avesse i poli coincidenti, sarebbe quindi della forma

$$z' = z + \beta.$$

Ma una tale sostituzione, ripetuta m volte, dà

$$z' = z + m\beta$$

e, non avendo periodo finito, non può far parte di un gruppo finito.

§. 44. — Supponiamo di avere m sostituzioni lineari

$$\psi_i(z) = \frac{a_i z + b_i}{c_i z + d_i} \quad (i = 1, 2, 3 \ldots m) \tag{3}$$

che formino un gruppo finito G. Fra le (3) figurerà naturalmente l'identità; supponiamo che sia

$$\begin{pmatrix} a_1 , & b_1 \\ c_1 , & d_1 \end{pmatrix} = \begin{pmatrix} 1 , & 0 \\ 0 , & 1 \end{pmatrix} ,$$

cioè $\psi_1(z) = z$. Ciascuna delle $m-1$ sostituzioni rimanenti ha *due* poli distinti, onde il numero totale N dei poli delle sostituzioni di G sarà

$$N = 2(m-1),$$

quando naturalmente si conti ogni polo tante volte quante sono le sostituzioni del gruppo, esclusa l'identità, che lo hanno per punto fisso.

Sia ora $z = k$ un polo comune a ν sostituzioni di G, l'identità compresa, e siano

$$\psi_1(z),\ \psi_2(z) \ldots \psi_\nu(z) \tag{4}$$

queste ν sostituzioni, talchè sia:

$$k = \psi_1(k),\ k = \psi_2(k) \ldots k = \psi_\nu(k).$$

Segue subito da ciò che le ν sostituzioni (4) formano un sottogruppo di G; poichè da

$$k = \psi_i(k),\ k = \psi_j(k)$$

segue anche

$$k = \psi_i(\psi_j(k)).$$

Ma ora dimostriamo l'importante teorema:

Il sottogruppo Γ *di* G *formato dalle* ν *sostituzioni* (4), *che hanno un polo* k *a comune, è un gruppo ciclico, cioè è formato dalle potenze di una conveniente sostituzione* (4) *a periodo* ν.

Cangiando linearmente z, si può intanto trasportare il polo k in $z = \infty$, dopo di che le (4) assumeranno la forma

$$\psi_1(z) = z,\ \psi_2(z) = \varepsilon_i z + c_i\ (i = 2, 3, \ldots \nu). \tag{4*}$$

Ripetendo ν volte una qualunque di esse, deve ottenersi l'identità e però si ha

$$\varepsilon_i^\nu = 1,$$

cioè i moltiplicatori

$$\varepsilon_1 = 1,\ \varepsilon_2,\ \varepsilon_3 \ldots \varepsilon_\nu$$

delle sostituzioni (4*) sono tutti radici ν^{me} dell'unità e, se proviamo che sono tutti diversi fra loro, saranno le potenze di una medesima radice primitiva ν^{ma} dell'unità. Intanto, cangiando z in z + costante, possiamo rendere una delle c p. e. $c_2 = 0$; dico allora che ogni altra c p. e. c_3 risulterà nulla. Infatti da

$$\psi_2(z) = \varepsilon_2 z,\ \psi_3(z) = \varepsilon_3 z + c_3$$

deduciamo

$$\psi_2(\psi_3(z)) = \varepsilon_2 \varepsilon_3 z + \varepsilon_2 c_3$$

$$\psi_3(\psi_2(z)) = \varepsilon_2 \varepsilon_3 z + c_3$$

e, componendo la prima coll'inversa della seconda, avremmo in Γ la sostituzione

$$z' = z + \frac{(\varepsilon_2 - 1) c_3}{\varepsilon_2 \varepsilon_3}$$

che non avrebbe periodo finito se non fosse $c_3 = 0$. Dopo ciò le sostituzioni (4) prenderanno la semplice forma

$$\psi_i(z) = \varepsilon_i z \quad (i = 1, 2, \ldots \nu),$$

onde le ε saranno tutte diverse fra loro, quindi potenze di una medesima $\varepsilon = e^{\frac{2\pi i}{\nu}}$, ciò che dimostra il teorema.

Risulta di più dalla nostra discussione:

Tutte le sostituzioni del sottogruppo ciclico Γ *hanno non solo il primo polo, ma anche il secondo a comune.*

Stabiliamo ora la nozione di *poli equivalenti*. Se k è un polo e ψ una qualunque sostituzione di G, sarà anche $k' = \psi(k)$ un polo e precisamente sarà polo comune alle sostituzioni del sottogruppo Γ' trasformato di Γ per mezzo di ψ.

I due poli k, k' si diranno allora equivalenti rispetto al gruppo G ed è chiaro che due poli equivalenti ad un terzo sono pure equivalenti fra loro, onde potremo ripartire i $2(m-1)$ poli in classi, ponendo nella medesima classe i poli equivalenti.

Essendo k un polo d'ordine ν, comune cioè a $\nu - 1$ sostituzioni di G, oltre l'identità, vediamo che nella classe di k vi sono precisamente $\frac{m}{\nu}$ poli tutti dell'ordine ν. E infatti in G vi sono ν sostituzioni soltanto, quelle del sottogruppo ciclico Γ, che lasciano fermo k, onde k è portato dalle sostituzioni di G in $\frac{m}{\nu}$ posti diversi (k compreso).

Se supponiamo dunque che i poli si ripartiscano in r classi con poli delle rispettive moltiplicità

$$\nu_1, \nu_2, \ldots \nu_r,$$

nella classe dei poli di moltiplicità ν_i avremo precisamente

$$\frac{m}{\nu_i}(\nu_i - 1)$$

poli. Dovremo quindi avere

$$\sum_{i=1}^{i=r} \frac{m}{\nu_i}(\nu_i - 1) = 2\,m - 2\,,$$

ovvero

$$\text{(A)} \qquad \sum_{i=1}^{i=r} \left(1 - \frac{1}{\nu_i}\right) = 2 - \frac{2}{m}\,.$$

È questa l'equazione fondamentale d'analisi indeterminata che ci servirà a risolvere il problema proposto.

§. 45. — Per trovare tutte le possibili soluzioni dell'equazione fondamentale (A) procederemo nel modo seguente [1]). In primo luogo osserviamo che il numero r sarà > 1 e non supererà 3. E invero se fosse $r = 1$ il primo membro della (A) sarebbe < 1, mentre il secondo, essendo $m \geq 2$, sarebbe ≥ 1. Nemmeno può essere $r \geq 4$, perchè il 1.° membro della (A), constando allora di 4 termini almeno ciascuno $\geq \frac{1}{2}$, sarebbe ≥ 2 mentre il 2.° membro è < 2. Dunque avremo necessariamente

$$r = 2 \text{ ovvero } r = 3\,.$$

1.° caso $r = 2$. La (A) diventa

$$\frac{1}{\nu_1} + \frac{1}{\nu_2} = \frac{2}{m}\,;$$

essendo ν_1, ν_2 divisori di m, si ha necessariamente

$$\nu_1 = \nu_2 = m.$$

Si ha dunque una prima soluzione della (A):

I) *m qualunque,* $\nu_1 = \nu_2 = m$.

2.° caso $r = 3$. La (A) diventa

$$\text{(B)} \qquad \frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3} = 1 + \frac{2}{m}\,.$$

---

[1]) Klein. — Ikosaeder.

Uno almeno dei tre numeri ν_1, ν_2, ν_3 deve essere $= 2$, perchè altrimenti il 1.° membro della (B) sarebbe ≤ 1. Facciamo dunque $\nu_1 = 2$ e rimarrà

$$\text{(C)} \qquad \frac{1}{\nu_2} + \frac{1}{\nu_3} = \frac{1}{2} + \frac{2}{m}.$$

Se un altro dei numeri ν è $= 2$, p. e. $\nu_2 = 2$, resta $\nu_3 = \frac{m}{2}$ e si ottiene una seconda soluzione della (A)

II) $m = 2n$; $\nu_1 = 2$, $\nu_2 = 2$, $\nu_3 = n$ *(n qualunque).*

Siano in fine $\nu_2 > 2$, $\nu_3 > 2$; allora uno dei due sarà $= 3$, perchè se fosse $\nu_2 > 3$, $\nu_3 > 3$ il 1.° membro della (C) sarebbe $\leq \frac{1}{2}$. Poniamo dunque che sia $\nu_2 = 3$ e rimarrà

$$\frac{1}{\nu_3} = \frac{1}{6} + \frac{2}{m},$$

per cui sarà certamente $\nu_3 < 6$ e facendo successivamente

$$\nu_3 = 3, 4, 5,$$

troviamo le nuove soluzioni

$$\text{(III)} \qquad m = 12;\ \nu_1 = 2,\ \nu_2 = 3,\ \nu_3 = 3$$

$$\text{(IV)} \qquad m = 24;\ \nu_1 = 2,\ \nu_2 = 3,\ \nu_3 = 4$$

$$\text{(V)} \qquad m = 60;\ \nu_1 = 2,\ \nu_2 = 3,\ \nu_3 = 5.$$

Così sono trovate tutte le possibili soluzioni della (A). Dimostreremo poi che a ciascuna di esse corrisponde uno ed un sol tipo di gruppi di sostituzioni lineari. Questi gruppi, per una ragione che fra breve si vedrà, portano i seguenti nomi:

Tipo I) gruppi ciclici (o della piramide regolare).
Tipo II) gruppi diedrali (o della doppia piramide).
Tipo III) gruppo del tetraedro.
Tipo IV) gruppo dell'ottaedro (o del cubo).
Tipo V) gruppo dell' isocaedro (o del dodecaedro).

§. 46. — Possiamo subito procedere alla effettiva costruzione dei gruppi dei primi due tipi.

In un gruppo G_n del primo tipo d'ordine n, avendosi $\nu_1 = \nu_2 = n$, esiste (§. 44) una sostituzione S a periodo n e il gruppo G_n è il gruppo ciclico

$$G_n = (1, S, S^2, \ldots S^{n-1}).$$

Alla sostituzione S, cangiando linearmente la variabile, si può dare la forma normale (§. 44)

$$z' = \varepsilon z,$$

essendo ε una radice primitiva n^{ma} dell'unità. Dunque: *Un gruppo del tipo I) si può rappresentare analiticamente così:*

$$a) \qquad z' = z, \; z' = \varepsilon z, \; z' = \varepsilon^2 z, \ldots z' = \varepsilon^{n-1} z$$

$$\varepsilon = e^{\frac{2\pi i}{n}}.$$

Consideriamo ora un gruppo G_m del tipo II) con

$$m = 2n, \; \nu_1 = \nu_2 = 2, \; \nu_3 = n$$

A causa di $\nu_3 = n$ esso possiede un sottogruppo Γ_n d'ordine n del tipo I), cui potremo dare la forma normale a).

Sia ora T una sostituzione di G_{2n} fuori di Γ; avendosi

$$G = (\Gamma, T\,\Gamma)$$

come anche

$$G = (\Gamma, \Gamma\,T)$$

sarà necessariamente $ST = TS^r$ per un conveniente valore di r, cioè

$$T^{-1} S T = S^r.$$

Se supponiamo che sia

$$z' = \frac{\alpha z + \beta}{\gamma r + \delta}$$

l'espressione analitica di T, dovremo avere identicamente

$$\frac{\alpha \varepsilon z + \beta}{\gamma \varepsilon z + \delta} = \varepsilon^r \frac{\alpha z + \beta}{\gamma z + \delta},$$

onde risulta

$$\alpha = \delta = 0,$$

ovvero $\beta = \gamma = 0$. L'ultimo caso è da escludersi perchè allora T avrebbe come S la forma moltiplicativa

$$z' = k z$$

e conseguentemente (§. 44) G_{2n} sarebbe un gruppo ciclico, cioè del tipo I). La T avrà dunque la forma

$$z' = \frac{k}{z}$$

e mutando z in $a z$, ciò che non altera la forma $z' = \varepsilon z$ di S, potremo dare a k un valore fisso qualunque p. e. $k = -1$. Così dunque: *Un gruppo del tipo II) d'ordine* $2n$ *si può porre sotto la forma normale*

$$b) \qquad z' = \varepsilon^r z\,,\ z' = -\frac{\varepsilon^r}{z} \begin{cases} \varepsilon = e^{\frac{2\pi i}{n}} \\ r = 0, 1, 2 \ldots n-1 \end{cases} .$$

Queste $2n$ sostituzioni b) formano inversamente, come è chiaro, un gruppo del tipo II).

Per la costruzione dei gruppi dei tre tipi rimanenti è utile che dimostriamo ora il teorema seguente:

Se un gruppo G *di sostituzioni lineari sopra una variabile contiene un sottogruppo ciclico* Γ *invariante, il gruppo* G *stesso appartiene al primo od al secondo tipo.*

Possiamo supporre che sia Γ il *più ampio* sottogruppo ciclico invariante di G. A questo gruppo Γ daremo la forma normale a)

$$z' = \varepsilon^r z\,.$$

Ogni sostituzione di G, dovendo trasformare Γ in se medesimo, avrà, per quanto sopra si è visto, l'una o l'altra delle due forme

$$z' = a z\,,\ z' = \frac{k}{z}\,.$$

Se vi fossero in G sostituzioni della 1.ª forma, oltre quelle di Γ, le sostituzioni di G di questa forma moltiplicativa formerebbero un sottogruppo ciclico invariante più ampio di Γ contro l'ipotesi. D'altronde se T, T′ sono due sostituzioni di G fuori di Γ:

$$\mathrm{T})\ z' = \frac{k}{z} \qquad \mathrm{T'})\ z' = \frac{k'}{z}$$

la TT' ha la forma moltiplicativa

$$z' = \frac{k'}{k} z$$

ed è quindi in Γ. Dunque tutte le sostituzioni di G si ordinano nel quadro

$$G = \begin{cases} 1, & S, & S^2 \ldots & S^{n-1} \\ T, & TS, & TS^2, \ldots & TS^{n-1} \end{cases}$$

e G appartiene quindi al secondo tipo.

§. 47. — *Gruppo del tetraedro.* Per un gruppo del tipo III) abbiamo

$$m = 12\,,\ \nu_1 = 2\,,\ \nu_2 = 3\,,\ \nu_3 = 3\,.$$

In questo gruppo del 12.° ordine il numero dei sottogruppi del 3.° ordine, a causa del teorema di Sylow, sarà 1 o 4. Il primo caso si esclude subito perchè allora G_{12} conterrebbe un Γ_3 invariante e apparterrebbe quindi al tipo I) o II). Avremo dunque in G_{12} quattro sottogruppi

$$H_1\ H_2\ H_3\ H_4$$

del 3.° ordine che, trasformati con tutte le sostituzioni di G_{12} darannno luogo ad un gruppo Γ transitivo sui 4 elementi H col quale G_{12} sarà isomorfo. Ora l'isomorfismo non può essere meriedrico, perchè se n è il grado di meriedria, deve essere $\frac{12}{n}$ (ordine di Γ) multiplo di 4, onde

$$n = 3 \text{ o } n = 1\,.$$

Nel primo caso il sottogruppo Σ di G cui corrisponde l'indentità in Γ sarebbe ciclico del 3.° ordine ed invariante in G, ciò che è impossibile. Dunque $n = 1$ e Γ è il gruppo alterno sui quattro elementi H. Se prendiamo le tre sostituzioni di Γ

$$(H_1\ H_2\ H_3)$$
$$(H_1\ H_4)\ (H_2\ H_3)$$
$$(H_1\ H_2)\ (H_3\ H_4)\,,$$

colle quali tutto Γ si genera, basterà costruire in G_{12} le tre corrispon-

denti che indicheremo con S, T, T'. Significheremo questa corrispondenza colle segnature

$$S \sim (H_1\, H_2\, H_3)$$
$$T \sim (H_1\, H_4)\ (H_2\, H_3)$$
$$T' \sim (H_1\, H_2)\ (H_3\, H_4)$$

Alla T di periodo 2 potremo dare, cangiando linearmente z, la forma normale (§. 44)

$$\text{T)}\ z' = -z.$$

Ora si ha $TT' = T'T$ [1]) e però T' ha la forma moltiplicativa $z' = az$, ovvero l'altra $z' = \frac{k}{z}$. Il 1.° caso è subito escluso perchè T' essendo a periodo 2 sarebbe $a^2 = 1$ e T' coinciderebbe con T. Mutando z in λz, si serba a T la medesima forma e si può fare, nell'espressione di T', $k = 1$, cioè:

$$\text{T')}\ z' = \frac{1}{z}.$$

Se poniamo

$$T'' = TT' \sim (H_1\, H_3)\ (H_2\, H_4),$$

avremo quindi

$$\text{T'')}\ z' = -\frac{1}{z}.$$

Sia ora

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta}$$

la forma di S. Osservando che si ha

$$TS = ST'',\quad T'S = ST,$$

ne deduciamo le identità

$$\frac{\alpha z - \beta}{\gamma z - \delta} = -\frac{\gamma z + \delta}{\alpha z + \beta},\quad \frac{\alpha + \beta z}{\gamma + \delta z} = -\frac{\alpha z + \beta}{\gamma z + \delta},$$

---

[1]) Per verificare le relazioni fra S, T, T' di cui ci serviamo nel testo basta verificarle, a causa dell' isomorfismo oloedrico fra G, Γ, sulle sostituzioni corrispondenti a destra.

da cui

$$\alpha^2 + \gamma^2 = 0\,,\ \beta^2 + \delta^2 = 0$$
$$\alpha\delta + \beta\gamma = 0\,,\ \beta\delta + \alpha\gamma = 0\,.$$

Ne seguono le formole

$$\beta = \pm\alpha\,,\ \gamma = i^{\varepsilon}\alpha\,,\ \delta = \mp i^{\varepsilon}\alpha\,,$$

avendo ε il valore 1 o 3. La S avrà dunque una delle quattro forme

$$i\frac{z+1}{z-1}\,,\quad i\frac{z-1}{z+1}\,,\quad -i\frac{z+1}{z-1}\,,\quad -i\frac{z-1}{z+1}\,.$$

E siccome una qualunque di queste quattro sostituzioni, combinata con T, T', T'', dà le altre tre ne concludiamo che il gruppo cercato G_{12} le contiene tutte. Abbiamo così ottenuto pel gruppo del tetraedro la forma normale:

$$c)\qquad z' = \pm z\,,\ \pm\frac{1}{z}\,,\ \pm i\frac{z+1}{z-1}\,,\ \pm i\frac{z-1}{z+1}\,,\ \pm\frac{z+i}{z-i}\,,\ \pm\frac{z-i}{z+i}\,.$$

Si riscontra subito in effetto che queste 12 sostituzioni formano il gruppo domandato.

§. 48. — *Gruppo dell'ottaedro.* Un gruppo G del 4.° tipo contiene 24 sostituzioni e quindi un certo numero di sottogruppi del 3.° ordine che, servendosi del teorema di Sylow, si riscontra subito nuovamente essere $= 4$; siano

$$H_1\, H_2\, H_3\, H_4$$

questi sottogruppi. Per trasformazione con le sostituzioni di G si ottiene ancora un gruppo Γ sui quattro elementi H, col quale G è isomorfo. Anche qui l'isomorfismo è oloedrico. Invero il grado n del sottogruppo Σ in G che corrisponde all'identità in Γ, dovendo essere un divisore di 6, potrebbe offrire i casi

$$n = 6\,,\ n = 3\,,\ n = 2\,,\ n = 1\,.$$

I casi $n = 3$, $n = 2$ sono immediatamente esclusi, giacchè Σ sarebbe ciclico. Ma nemmeno può essere $n = 6$, perchè Σ conterrebbe *un solo* sottogruppo del 3.° ordine invariante quindi non solo in Σ, ma anche in G. Ne concludiamo che G è oloedricamente isomorfo col gruppo totale Γ_{24} sui quattro elementi H; esso contiene dunque un sottogruppo G_{12}, cor-

rispondente al gruppo alterno che è necessariamente del tipo III) [1]) e potremo quindi già supporre ridotto alla forma normale *c*) del §. precedente. Per determinare completamente le sostituzioni di G basterà costruirne una fuori del sottogruppo tetraedrale. Scegliamo la seguente

$$U \sim (H_1\, H_2\, H_4\, H_3)\,,$$

che essendo permutabile con $T \sim (H_1\, H_4)\,(H_2\, H_3)$ avrà o la forma moltiplicativa

$$z' = a\, z$$

o l'altra $z' = \frac{k}{z}$. Questa seconda però resta subito esclusa perchè U sarebbe allora a periodo 2, mentre è a periodo 4. Si ha dunque per la U

$$z' = \pm\, i\, z\,.$$

Il segno è indifferente perchè l'una sostituzione nasce dall'altra combinata con T. Dunque per la forma normale dei gruppi del IV.° tipo abbiamo

$$d) \qquad z' = i^{\varepsilon}\, z\,,\ \frac{i^{\varepsilon}}{z}\,,\ i^{\varepsilon}\,\frac{z \pm 1}{z \mp 1}\,,\ i^{\varepsilon}\,\frac{z \pm i}{z \mp i}\ (\varepsilon = 0, 1, 2, 3).$$

Queste 24 sostituzioni formano in effetto il gruppo richiesto.

§. 49 — Per costruire i gruppi dell'ultimo tipo, cominciamo dal dimostrare che: *Un gruppo* G_{60} *del V.° tipo è un gruppo semplice.*

Esso non può certamente contenere come sottogruppo invariante un gruppo ciclico (§. 46); ma è facile vedere che non può contenere nemmeno come invariante un gruppo G_{2n} del tipo II), se pure escludiamo per un momento il caso $n = 2$. E infatti un tale gruppo contiene un solo sottogruppo ciclico d'ordine n, che sarebbe dunque esso stesso invariante in G_{60}. Se Γ_m è un sottogruppo invariante di G_{60}, e non è diedrale con $m = 4$, sarà dunque necessariamente $m = 12$ poichè è questo l'unico divisore di 60 che possa essere ordine di un gruppo non ciclico nè diedrale. Dunque si avrebbe in G_{60} un sottogruppo invariante tetrae-

---

[1]) Se fosse diedrale dovrebbe contenere una sostituzione a periodo 6, ciò che non è (Cf. anche le osservazioni al principio del seguente §).

drale G_{12}; d'altronde questo contiene un solo sottogruppo diedrale Γ_4 che sarà ancora invariante in G_{60}. Basterà dunque ricercare se tale caso può darsi. Possiamo dare alle sostituzioni di Γ_4 la forma

$$\Gamma_4) z' = z\,,\ z' = -z\,,\ z' = \frac{1}{z}\ z' = -\frac{1}{z}\ .$$

Ora se S è una sostituzione di G_{60} a periodo 5, trasformando con S le tre sostituzioni di Γ_4 diverse dall'identità, queste o resteranno singolarmente invariate o si scambieranno fra loro secondo una sostituzione a periodo 5. Quest'ultima circostanza non può darsi perchè non esiste una sostituzione a periodo 5 su tre lettere. Dunque la S sarebbe permutabile colle tre dette sostituzioni di Γ_ε, ciò che subito si vede essere impossibile, poichè essendo S permutabile con $z' = -z$ e non avendo il periodo 2 ma 5, avrebbe la espressione $z' = \varepsilon z$ con ε radice quinta dell'unità; ma allora non è più permutabile coll'altra $z' = \frac{1}{z}$.

Di qui e dal teorema al §. 29 risulta che il gruppo G_{60} da costruirsi, essendo semplice, è oloedricamente isomorfo col gruppo alterno su 5 lettere

$$a,\ b,\ c,\ d,\ e.$$

Basterà qnindi costruire le sostituztoni S, T, U di G_{60} corrispondenti alle sostituzioni seguenti del gruppo alterno

$$\begin{aligned} S &\sim (a\,b\,c\,d\,e) \\ T &\sim (b\,c)\ (d\,e) \\ U &\sim (b\,e)\ (d\,c)\,, \end{aligned}$$

delle quali le prime due bastano già a generare tutto il gruppo alterno [1]).

---

[1]) Pongasi infatti

$$A = (a\,b\,c\,d\,e)\,,\ B = (b\,c)\ (d\,e)\,,\ C = (b\,e)\ (c\,d)\,;$$

si ha

$$B\,A = (a\,b\,d)\,,\ C = A^2\,B\,A^3\,B\,A^2\,B\,.$$

Il gruppo generato da A, B contiene dunque una sostituzione del 5.° ordine A, una del 3.° B A e il gruppo del 4.° ordine

$$1,\ B,\ C,\ B\,C,$$

onde il suo ordine è multiplo di $4 \times 5 \times 3$ e però $= 60$.

Alla sostituzione ciclica del 5.° ordine S potremo dare la forma normale (§. 44):

$$\text{S)}\ z' = \varepsilon z \ \text{con}\ \varepsilon = e^{\frac{2\pi i}{5}},$$

cangiando eventualmente la denominazione delle lettere a, b, c, d, e. Si abbia ora per U

$$\text{U)}\ z' = \frac{\alpha z + \beta}{\gamma z + \delta};$$

essendo

$$U^{-1} S U = S^4, \ \text{cioè}\ S U = U S^4,$$

dovremo avere l'identità

$$\frac{\alpha \varepsilon z + \beta}{\gamma \varepsilon z + \delta} = \varepsilon^4 \frac{\alpha z + \beta}{\gamma z + \delta},$$

indi

$$\alpha \gamma = 0, \ \beta \delta = 0, \ \alpha \delta = 0$$

e poichè, a causa dell'ultima, deve essere $\beta \gamma \neq 0$, avremo

$$\alpha = 0 \quad \delta = 0$$

e la U avrà la forma

$$z' = \frac{k}{z}.$$

Cangiando z in λz, ciò che non altera la S, possiamo fare $k = -1$, cioè

$$\text{U)}\ z' = -\frac{1}{z}.$$

Si abbia infine per la T

$$\text{T)}\ z' = \frac{a z + b}{c z + d}.$$

Essendo $T^2 = \begin{pmatrix} a^2+bc, & b(a+d) \\ c(a+d) & a^2+bc \end{pmatrix} = 1$, ne risulta

$$a + d = 0.$$

Inoltre da $T U = U T$ abbiamo

$$-\frac{c z + d}{a z + b} = \frac{b z - a}{d z - c},$$

onde

$$a\,b + c\,d = 0\,,\quad a^2 + c^2 = b^2 + d^2\,.$$

Avremo dunque

$$d = -a \quad b = c\,,$$

a meno che non sia $a = d = 0$, $b = -c$; ma questo caso è da escludersi perchè T coinciderebbe allora con U. Dunque si ha per T

$$\text{T)}\ z' = \frac{a\,z + b}{b\,z - a}\,.$$

Ora facciamo uso dell'identità

$$\text{U} = \text{S}^2\,\text{T}\ \text{S}^3\,\text{T}\ \text{S}^2\,\text{T}\,,$$

che scriviamo

$$\text{U}\,\text{T} = \text{S}^2\,\text{T}\ \text{S}^3\,\text{T}\ \text{S}^2\,,$$

e ne ricaviamo

$$\frac{a - b\,z}{a\,z + b} = \frac{(\varepsilon^2\,a^2 + \varepsilon^4\,b^2)\,z + (1 - \varepsilon^2)\,a\,b}{(1 - \varepsilon^2)\,a\,b\,z + (\varepsilon^3\,b^2 + a^2)}\,,$$

da cui

$$a^2\,(1 + \varepsilon^2) + b^2\,(\varepsilon^3 + \varepsilon^4) = 0$$

cioè

$$\frac{a^2}{b^2} = -\frac{\varepsilon^3 + \varepsilon^4}{1 + \varepsilon^2}\,.$$

A causa della identità

$$\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0\,,$$

possiamo scrivere

$$\frac{a^2}{b^2} = \frac{(\varepsilon^4 - \varepsilon)^2}{(\varepsilon^2 - \varepsilon^3)^2}\,,$$

Possiamo dunque porre $a = \varepsilon^4 - \varepsilon$, $b = \pm\,(\varepsilon^2 - \varepsilon^3)$ e siccome, cangiando z in $-z$, non si alterano S, U, mentre cangia in T il segno di b, possiamo prendere senz'altro

$$\text{T)}\ z' = \frac{(\varepsilon^4 - \varepsilon)\,z + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3)\,z - (\varepsilon^4 - \varepsilon)}\,.$$

Combinando S, T, U e le loro potenze, ne concludiamo che ai gruppi del tipo V), o dell'icosaedro, si può dare la forma normale

$$e)\ z' = \varepsilon^r\,z,\ -\frac{\varepsilon^r}{z},\ \varepsilon^r\,\frac{(\varepsilon^4 - \varepsilon)\,\varepsilon^s\,z + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3)\,\varepsilon^s\,z - (\varepsilon^4 - \varepsilon)}\,,\ \varepsilon^r\,\frac{(\varepsilon^4 - \varepsilon)\,\varepsilon^s\,z - (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3)\,\varepsilon^s\,z + (\varepsilon^4 - \varepsilon)}$$

$$r,\ s = 0,\ 1,\ 2,\ 3,\ 4.$$

È facile verificare direttamente che queste 60 sostituzioni formano in effetto un gruppo.

§. 50. — Le ricerche dei §§. precedenti ci hanno dimostrato come ad ogni soluzione dell'equazione fondamentale d'analisi indeterminata (A) §. 44 corrisponda uno ed *un solo* tipo di gruppi di sostituzioni lineari. Questi gruppi possono ricevere una notevolissima rappresentazione geometrica che li collega ai poliedri regolari e dà ragione del nome che hanno ricevuto di *gruppi dei poliedri regolari*. Per stabilire la indicata rappresentazione geometrica conviene prima che sostituiamo al piano di Gauss, come superficie sulla quale son distesi i valori della variabile complessa z, la *sfera complessa*, ciò che si fa nel modo seguente. Preso un sistema di assi cartesiani ortogonali $O\xi$, $O\eta$, $O\zeta$, distribuiamo, al modo di Gauss, sul piano $\xi\eta$ i valori della variabile complessa $z = x + iy$. Descriviamo poi, col centro nell'origine, la sfera di raggio $= 1$, che avrà per equazione

$$\xi^2 + \eta^2 + \zeta^2 = 1 ,$$

indi riportiamo, colla così detta *proiezione stereografica polare*, ogni punto $M \equiv (x, y)$ del piano equatoriale $\xi\eta$ in quel punto $M' \equiv (\xi, \eta, \zeta)$ della sfera che è allineato con M e col centro fisso di proiezione o *polo*

$$P \equiv (0, 0, 1).$$

Per tal modo i punti interni al cerchio equatoriale vengono proiettati sull'emisfero inferiore, quelli esterni sull'emisfero superiore, mentre i punti all'infinito del piano si raccolgono, in proiezione, nel polo P.

Faremo così corrispondere *biunivocamente* le posizioni di un punto sulla sfera ai valori della variabile complessa z e potremo, senza ambiguità, nominare un punto della sfera col corrispondente valore di z. La sfera rappresentativa si dirà, per abbreviare, la *sfera complessa;* i suoi due *poli* saranno il centro di proiezione $z = \infty$ ed il polo opposto $z = 0$.

Supponiamo ora che la sfera complessa, girando intorno al centro, si muova sopra se stessa; così ogni punto z andrà in una nuova posizione z' e nostro primo oggetto sarà di dimostrare il teorema fondamentale:

Ogni movimento della sfera complessa in se medesima è analiticamente rappresentato da una sostituzione lineare

$$z' = \frac{a z + b}{c z + d}$$

sulla variabile complessa. Queste sostituzioni lineari hanno del resto una forma speciale, come si vedrà nel prossimo §.

Volendo dimostrare questo teorema con mezzi affatto elementari, facciamo uso delle considerazioni seguenti.

I movimenti della sfera in se medesima sono operazioni suscettibili di composizione giacchè due movimenti, successivamente eseguiti, equivalgono ad un unico movimento composto. Ora diciamo che: *Qualunque movimento della sfera in se medesima può comporsi con tre successive rotazioni attorno ai tre assi coordinati* 0ξ, 0η, 0ζ.

Per dimostrarlo osserviamo che qualunque punto z_0 della sfera può essere trasportato con due successive rotazioni l'una attorno all'asse 0ξ, l'altra attorno all'asse 0η, nel polo $z = \infty$. E infatti basterà con una rotazione attorno a 0ξ portare dapprima z_0 nel piano meridiano $\xi\zeta$, indi con una rotazione attorno ad 0η si trasporterà nel polo $z = \infty$. Ciò posto, supponiamo che il movimento U trasporti il polo $z = \infty$ in z_0 e le due successive rotazioni T_ξ, T_η attorno agli assi 0ξ, 0η riconducano z_0 in $z = \infty$. Il movimento composto

$$U\, T_\xi\, T_\eta$$

lascerà fisso $z = \infty$ e per ciò anche il polo opposto $z = 0$, onde sarà una rotazione T_ζ attorno all'asse 0ζ. Avremo dunque

$$U\, T_\xi\, T_\eta = T_\zeta\,,$$

cioè

$$U = T_\zeta\, T_\eta^{-1}\, T_\xi^{-1}\,,$$

ciò che dimostra il teorema.

§. 51. — Per trovare la rappresentazione analitica di un movimento qualunque della sfera complessa in se medesima basterà, in ordine ai risultati precedenti, risolvere la questione per le rotazioni attorno agli assi coordinati. Cominciamo per ciò dal trovare le formole di *rappresentazione* stereografica polare, cioè le formole che legano le coordi-

nate x, y di un punto del piano equatoriale con quelle ξ, η, ζ del punto corrispondente sulla sfera. Poichè il punto $M \equiv (x, y, 0)$ è in linea retta coi due punti

$$P \equiv (0, 0, 1)\ ,\ M' \equiv (\xi, \eta, \zeta)$$

si troverà subito

$$(5) \qquad x = \frac{\xi}{1-\zeta}\,,\ y = \frac{\eta}{1-\zeta}\,,\ z = x + i\,y = \frac{\xi + i\,\eta}{1-\zeta}\,,$$

indi

$$(6) \qquad \xi = \frac{2\,x}{1+x^2+y^2}\,,\ \eta = \frac{2\,y}{1+x^2+y^2}\,,\ \zeta = \frac{x^2+y^2-1}{1+x^2+y^2}\,.$$

È utile dare a queste formole un altro aspetto introducendo, insieme a z, la variabile coniugata

$$z_0 = \frac{\xi - i\,\eta}{1-\zeta}\,;$$

allora le (6) diventano

$$(6^*) \qquad \xi = \frac{z+z_0}{z\,z_0+1}\,,\ \eta = \frac{1}{i}\,\frac{z-z_0}{z\,z_0+1}\,,\ \zeta = \frac{z\,z_0-1}{z\,z_0+1}\,.$$

Ciò premesso, consideriamo:

1.° *una rotazione nel senso positivo di ampiezza α attorno all'asse* $0\,\zeta$.

Indicando con (ξ', η', ζ') il punto in cui si trasporta (ξ, η, ζ) dopo il movimento, avremo

$$\begin{cases} \xi' = \xi \cos\alpha - \eta \operatorname{sen}\alpha \\ \eta' = \xi \operatorname{sen}\alpha + \eta \cos\alpha \\ \zeta' = \zeta \end{cases}$$

onde

$$z' = \frac{\xi' + i\eta'}{1-\zeta'} = \frac{(\cos\alpha + i \operatorname{sen}\alpha)(\xi + i\eta)}{1-\zeta} = e^{i\alpha}\,z\,,$$

formola che, dando al determinante della sostituzione il valore 1, converrà scrivere

$$(\alpha) \qquad z' = \frac{\cos\frac{\alpha}{2} + i \operatorname{sen}\frac{\alpha}{2}}{\cos\frac{\alpha}{2} - i \operatorname{sen}\frac{\alpha}{2}}\,z\,.$$

2.° *una rotazione d'ampiezza α, in senso positivo, attorno all'asse* $0\,\xi$.

Qui avremo

$$\begin{cases} \xi' = \xi \\ \eta' = \eta \cos\alpha - \zeta \operatorname{sen}\alpha \\ \zeta' = \eta \operatorname{sen}\alpha + \zeta \cos\alpha , \end{cases}$$

indi

$$z' = \frac{\xi + i\,(\eta \cos\alpha - \zeta \operatorname{sen}\alpha)}{1 - \eta \operatorname{sen}\alpha - \zeta \cos\alpha} ,$$

ossia per le (C*)

$$z' = \frac{z + z_0 + \cos\alpha\,(z - z_0) - i \operatorname{sen}\alpha\,(z z_0 - 1)}{z z_0 + 1 + i \operatorname{sen}\alpha\,(z - z_0) - \cos\alpha\,(z z_0 - 1)} .$$

Sopprimendo il fattore

$$2\left(\cos\frac{\alpha}{2} - i \operatorname{sen}\frac{\alpha}{2} z_0\right)$$

comune al numeratore e denominatore, troviamo

$$(\beta) \qquad z' = \frac{\cos\frac{\alpha}{2} \cdot z + i \operatorname{sen}\frac{\alpha}{2}}{i \operatorname{sen}\frac{\alpha}{2} z + \cos\frac{\alpha}{2}} .$$

3.° *una rotazione d'ampiezza* α *attorno all'asse* $O\eta$. Avremo qui

$$\begin{cases} \eta' = \eta \\ \zeta' = \zeta \cos\alpha - \xi \operatorname{sen}\alpha \\ \eta' = \zeta \operatorname{sen}\alpha + \xi \cos\alpha , \end{cases}$$

da cui

$$z' = \frac{\zeta \operatorname{sen}\alpha + \xi \cos\alpha + i\eta}{1 - \zeta \cos\alpha + \xi \operatorname{sen}\alpha} .$$

Sostituendo i valori (6*) e sopprimendo il fattore

$$2\left(\operatorname{sen}\frac{\alpha}{2} z_0 + \cos\frac{\alpha}{2}\right)$$

comune a numeratore e denominatore, avremo

$$(\gamma) \qquad z' = \frac{\cos\frac{\alpha}{2} z - \operatorname{sen}\frac{\alpha}{2}}{\operatorname{sen}\frac{\alpha}{2} z + \cos\frac{\alpha}{2}} .$$

Ora, pel teorema al §. 50, ogni movimento della sfera in sè componendosi con tre successive rotazioni rappresentate analiticamente da tre sostituzioni lineari (α), (β), (γ), è chiaro che anche la rappresentazione analitica di un tale movimento generale sarà data, come si enunciò al §. 50, da una sostituzione lineare

$$z' = \frac{Az + B}{Cz + D}.$$

Di più si osservi che in ciascuna delle sostituzioni elementari (α), (β), (γ) a determinante $= 1$ i coefficienti A, D sono coniugati mentre C è coniugato a $-B$, ossia indicando con A_0, B_0 le quantità coniugate di A, B si ha

$$z' = \frac{Az + B}{-B_0 z + A_0}, \quad A A_0 + B B_0 = 1,$$

e poichè due sostituzioni lineari di questa forma si compongono nuovamente in una sostituzione lineare della forma stessa, se ne conclude:

Qualunque movimento della sfera complessa in se medesima è rappresentato da una sostituzione lineare della forma

$$z' = \frac{A z_0 + B}{-B_0 z + A_0}, \quad A A_0 + B B_0 = 1.$$

La formola (I) così stabilita è la *formola di* Cayley.

In ogni movimento della sfera in se medesima, rappresentato dalla formola (I), vi sono due punti che rimangono fissi, quelli corrispondenti alle radici della equazione di 2.° grado

$$B_0 z^2 + (A - A_0) z + B = 0.$$

Ora se una radice di questa equazione è z l'altra è $-\frac{1}{z_0}$, come si vede cangiando i in $-i$, e siccome, per le (6*), per questo cangiamento ξ, η, ζ si mutano nei valori opposti $-\xi$, $-\eta$, $-\zeta$ si vede che in ogni tale movimento restano fissi due punti diametralmente opposti e il movimento non è che una rotazione attorno ad un diametro, proprietà ben nota.

È facile anche vedere inversamente che la formola (I) di Cayley, comunque si prendano le costanti A, B (con $A A_0 + B B_0 = 1$), rappresenta sempre un tale movimento. Per una tale sostituzione S infatti restano fissi, come si è visto, due punti diametralmente opposti che con un

effettivo movimento, rappresentato a sua volta da una sostituzione (I), sia T, possono trasportarsi nei poli $(0, \infty)$. La sostituzione trasformata $S_1 = T^{-1} S T$ lascia fissi i poli $0, \infty$ ed ha la forma (I) con $B = 0$ onde, essendo $A A_0 = 1$, potremo porre $A = e^{i\frac{\alpha}{2}}$ e la S_1 sarà per la (α) una rotazione attorno all'asse 0ζ, quindi

$$S = T S_1 T^{-1}$$

sarà ancora un movimento, come abbiamo asserito.

§. 52. — Insieme a quelle trasformazioni della sfera in se medesima che conservano l'eguaglianza *diretta* delle figure sferiche giova talora considerare quelle trasformazioni per le quali le figure corrispondenti sono inversamente eguali; una tale trasformazione si dirà un movimento *di 2.ª specie*. Per trovare la rappresentazione analitica di questi movimenti si osservi che la formola $z' = z_0$ rappresenta, per le (6*), un movimento di 2.ª specie e precisamente una simmetria rispetto al piano $\xi\,\zeta$. Combinando con questo il più generale movimento di 1.ª specie, dato dalla formola (I) di Cayley, avremo la formola

$$(\mathrm{I}^*) \qquad z' = \frac{A z_0 + B}{-B_0 z_0 + A_0}\,, \quad A A_0 + B B_0 = 1\,,$$

che ci rappresenta il più generale movimento di 2.ª specie. Fra questi movimenti (I*) meritano speciale attenzione quelli a periodo 2. Per trovarli osserviamo che l'inversa della (I*) è data da

$$z' = \frac{A z_0 - B_0}{B z_0 + A_0}$$

e coincide colla (I) solo quando si abbia

$$B = -B_0\,,$$

cioè quando B sia puramente immaginario, ovvero quando sia

$$A = 0\,, \; B = B_0 = \pm 1\,.$$

Nel 1.º caso cercando quali punti della sfera restano fissi, vediamo che essi debbono soddisfare l'equazione

$$B z z_0 + A_0 z - A z_0 + B_0 = 0\,,$$

cioè, ponendo

$$A = a_1 + i\,a_2\,,\quad B = i\,b$$

con a_1, a_2, b reali e $a_1^2+a_2^2+b^2 = 1$, all'altra

$$b(z\,z_0 - 1) - a_2(z + z_0) + \frac{a_1}{i}(z - z_0) = 0$$

che, osservando le (6*), diventa

$$(7)\qquad -a_2\,\xi + a_1\,\eta + b\,\zeta = 0\,,$$

equazione di un piano pel centro della sfera. Dunque: *In ogni movimento di 2.ª specie a periodo 2 della forma*

$$z' = \frac{A\,z_0 + i\,b}{i\,b\,z_0 + A_0}$$

rimangono fissi nella sfera tutti i punti del circolo massimo nel piano (7).

Perciò questo movimento non è che una *riflessione* su questo circolo.

Passiamo all'altro caso

$$A = A_0 = 0\,,\quad B = B_0 = \pm 1\,;$$

allora la sostituzione corrispondente

$$z' = -\frac{1}{z_0}$$

cangia ogni punto nel diametralmente opposto: essa si dirà *l'inversione.*

È bene osservare che: *In ogni movimento di 2.ª specie che non sia una riflessione nessun punto della sfera rimane fisso.*

Infatti, se rimanesse fisso un punto, lo stesso accadrebbe del diametralmente opposto e vi sarebbe un movimento affine che lascerebbe fissi i poli 0, ∞; ma quest'ultimo movimento è rappresentato da

$$z' = \frac{A}{A_0}\,z_0$$

ed è per ciò una riflessione.

§. 53 — Se un certo numero di rotazioni della sfera complessa in se medesima formano un gruppo, formeranno pure un gruppo (oloedricamente isomorfo) le sostituzioni lineari che li rappresentano secondo la formola (I) di Cayley. Un tale gruppo, quando consti di un numero fi-

nito di operazioni, dovrà necessariamente rientrare in uno dei cinque tipi studiati nei precedenti §§. Dimostreremo ora direttamente la esistenza di gruppi di rotazioni di ciascuno dei cinque tipi e stabiliremo così la rappresentazione geometrica cercata [1]).

Consideriamo un poligono regolare inscritto o circoscritto alla sfera complessa. Con una rotazione attorno al centro possiamo sovrapporre il poliedro a se medesimo e precisamente possiamo portare uno spigolo fisso del poliedro sovra un altro spigolo qualunque in *due* modi diversi. Il numero N di queste rotazioni distinte (l'identità compresa) è quindi eguale al doppio del numero degli spigoli ed è evidente che queste rotazioni formano un gruppo, perchè sono tutte e sole quelle che riportano il poliedro in se stesso [2]).

Dei cinque poliedri regolari basta considerarne tre soltanto poichè due poliedri polari l'uno dell'altro, cioè l'ottaedro o il cubo e l'icosaedro o il dodecaedro, danno luogo al medesimo gruppo, come si riconosce subito osservando che i piani tangenti nei vertici di un poliedro iscritto sono le faccie del poliedro polare. Avremo quindi tre gruppi di rotazioni corrispondenti rispettivamente al tetraedro, all'ottaedro ed all'icosaedro con 12, 24 e 60 rotazioni; questi sono, come ora verificheremo, i gruppi dei tipi III), IV), V). Ma possiamo anche facilmente trovare i gruppi di rotazioni corrispondenti ai tipi I) e II). Si considerino perciò i solidi seguenti:

1.° *una piramide regolare con un numero qualunque n di facce laterali, la cui base sia inscritta nel circolo equatoriale, e col vertice nel polo $z = \infty$ della sfera.*

2.° *una doppia piramide regolare ottenuta riunendo alla precedente piramide la simmetrica rispetto al piano equatoriale.*

Il primo solido si sovrappone a se medesimo per un gruppo (ciclico) di rotazioni, che ha una rotazione generatrice S d'amplitudine $= \frac{2\pi}{n}$ attorno all'asse polare.

---

[1]) Potremmo dedurre il risultato anche dalle forme normali date ai gruppi dei cinque tipi poichè le loro sostituzioni, ridotte a determinante $= 1$, acquistano appunto la forma (I) di Cayley.

[2]) L'ordine N di questo gruppo si può anche valutare dal numero f delle facce supposte m — latere o da v dei vertici con angoli solidi n — lateri; si avrà

$$N = fm = vn = 2s\,.$$

Il secondo solido, oltre che dalle precedenti rotazioni, è ricondotto in se stesso dalle n rotazioni d'ampiezza $= \pi$ (ribaltamenti) attorno agli assi che dal centro vanno ai vertici ed ai punti medii dei lati della base comune delle due piramidi.

I gruppi corrispondenti appartengono appunto, come è chiaro, ai tipi I) II).

§. 54. — Esaminiamo ora come nei gruppi di rotazioni dei tre poliedri regolari si realizzano geometricamente tutte le circostanze che già nell'enumerazione dei vari tipi di gruppi abbiamo analiticamente riconosciuto.

Il gruppo tetraedrale consta di $2 \times 6 = 12$ rotazioni fra le quali figurano 3 rotazioni a periodo 2 attorno alle tre congiungenti i punti medii delle costole opposte; queste tre congiungenti incontrano la sfera in 6 punti che figurano appunto come i poli di 2.° ordine corrispondenti a $\nu_1 = 2$. Abbiamo poi 8 rotazioni a periodo 3 attorno alle quattro congiungenti i vertici coi punti medii delle facce opposte e i poli di queste rotazioni si dividono in due classi di poli equivalenti, cioè: i 4 vertici ed i 4 punti diametralmente opposti, corrispondentemente ai valori $\nu_2 = 3$, $\nu_3 = 3$.

L'isomorfismo del gruppo tetraedrale col gruppo alterno su quattro elementi è reso qui evidente dal fatto che i quattro vertici (o le quattro facce) vengono permutati fra loro in 12 modi diversi dalle rotazioni del gruppo. Si può anche rappresentare analiticamente il gruppo sui quattro vertici, distinti cogli indici

$$\infty, 0, 1, 2$$

come gruppo modulare per $p = 3$ (§. 41)

$$\nu' \equiv \frac{\alpha\nu + \beta}{\gamma\nu + \delta}, \quad \alpha\delta - \beta\gamma \equiv 1 \pmod 3.$$

Scrivendo per disteso le 12 sostituzioni abbiamo:

rotazioni a periodo 3 (sostituzioni paraboliche)

$$\nu' \equiv \nu + 1, \quad \nu + 2, \quad \frac{\nu}{\nu+1}, \quad \frac{\nu}{2\nu+1}, \quad \frac{2}{\nu+1}, \quad \frac{\nu+1}{2\nu}$$

$$(0\,1\,2), \quad (0\,2\,1), \quad (\infty\,1\,2), \quad (\infty\,2\,1), \quad (0\,2\,\infty), \quad (0\,\infty\,2)$$

rotazioni a periodo 2 (sostituzioni iperboliche)

$$\nu' \equiv -\frac{1}{\nu}\ , \quad \frac{1-\nu}{1+\nu}\ , \quad \frac{1+\nu}{-1+\nu}$$

$$(0\,\infty)(1\,2)\ ,(0\,1)(2\,\infty),(0\,2)(1\,\infty).$$

Queste ultime tre, che sono ribaltamenti attorno a tre assi ortogonali concorrenti nel centro, formano insieme all'identità il sottogruppo G_4 [1]) invariante in G_{12}.

Passiamo al gruppo dell'ottaedro o cubo. Riferendoci p. e. al cubo, avremo 9 rotazioni di periodo 4 o 2 attorno alle tre congiungenti i centri delle facce opposte, 8 rotazioni a periodo 3 attorno alle quattro diagonali, 6 rotazioni a periodo 2 attorno alle congiungenti i punti medii delle costole parallele opposte. Queste $9+8+6$ rotazioni, insieme all'identità, esauriscono le 24 rotazioni del gruppo. Le quattro diagonali vengono permutate dal gruppo di rotazioni in 24 modi diversi, Abbiamo così l'immagine geometrica dell'isomorfismo (oloedrico) del gruppo ottaedrale col gruppo totale su quattro elementi, ovvero col gruppo lineare totale

$$\nu' \equiv \frac{\alpha\nu+\beta}{\gamma\nu+\delta} \pmod 3.$$

Osserviamo poi che considerando un vertice A del cubo e sulle tre facce che vi concorrono i tre vertici opposti, questi quattro vertici sono vertici altresì di un tetraedro regolare inscritto nel cubo; i rimanenti quattro vertici determinano medesimamente un secondo tetraedro regolare. Le 24 rotazioni del gruppo ottaedrale lasciano fermo ciascuno dei due tetraedri ovvero li scambiano fra loro secondo che, come sostituzioni sulle quattro diagonali, sono pari o dispari. Le prime, in numero di 12, formano il sottogruppo invariante tetraedrale.

§. 55. — L'icosaedro ha 12 vertici, 20 facce e 30 spigoli. Il suo gruppo consta di 60 rotazioni che si ripartiscono nel modo seguente:

1.° 24 rotazioni a periodo 5 attorno alle 6 congiungenti i vertici opposti (diametri dell'icosaedro).

2.° 20 rotazioni a periodo 3 attorno alle 10 congiungenti i centri delle facce parallele opposte.

---

[1]) Vierergruppe, secondo le denominazioni di Klein.

3.° 15 rotazioni a periodo 2 attorno alle 15 congiungenti i punti medii delle costole parallele opposte.

4.° l'identità:

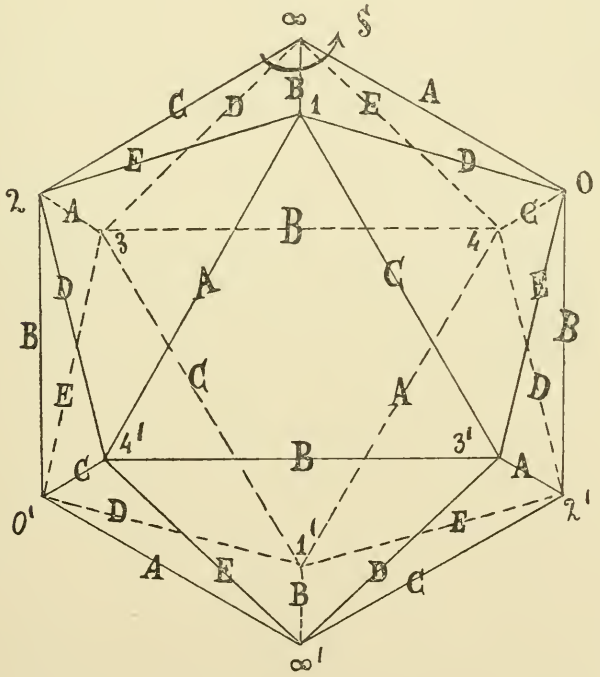
$$24 + 20 + 15 + 1 = 60.$$

I sei diametri dell'icosaedro vengono permutati fra loro secondo 60 sostituzioni di un gruppo transitivo semplice, che coincide dunque col gruppo modulare per $p = 5$. Ciò confermiamo geometricamente così. Distinguiamo i 6 diametri dell'icosaedro cogli indici

$$\infty, 0, 1, 2, 3, 4,$$

come è indicato nella figura 1.ª

Fig. 1.



pei vertici corrispondenti e consideriamo la rotazione S di ampiezza $= \frac{2\pi}{5}$ attorno al diametro $\infty\ \infty'$ nel senso della freccia e il ribaltamento T attorno alla congiungente i punti medii degli spigoli opposti $\overline{\infty\, 0}$, $\overline{\infty'\, 0'}$. Sopra i sei diametri la S produce la sostituzione

$$(0\ 1\ 2\ 3\ 4) \text{ ossia } \nu' \equiv \nu + 1 \pmod 5$$

e la T l'altra

$$(0\,\infty)\,(14) \text{ ovvero } \nu' \equiv -\frac{1}{\nu} \mod (5)$$

che sono le sostituzioni generatrici del gruppo modulare (§. 41) e però colle due rotazioni S, T si genera tutto il gruppo dell' icosaedro, come è anche facile vedere geometricamente.

Si osservi poi che l'isomorfismo del gruppo icosaedrale col gruppo alterno su 5 elementi risulta direttamente sulla figura nel modo seguente. I 30 spigoli dell'icosaedro possono ripartirsi in 5 sistemi, di 6 spigoli ciascuno, in guisa che ogni sistema consti di due terne ortogonali, gli spigoli di una terna essendo paralleli a quelli dell'altra, Per ottenere questa distribuzione degli spigoli in sistemi basta osservare la piramide regolare a base pentagonale che si forma ad ogni angolo solido dell'icosaedro; ad ogni lato (spigolo) del pentagono base appartiene, nel medesimo sistema, lo spigolo laterale opposto. Distinguendo i cinque sistemi colle lettere

$$A,\ B,\ C,\ D,\ E$$

viene attribuita, nella fig. 1.ª, ad ogni spigolo la lettera del sistema cui appartiene. Vediamo allora che le rotazioni elementari S, T del gruppo icosaedrale producono sui cinque sistemi A, B, C, D, E le sostituzioni elementari del gruppo alterno

$$S \sim (A\ B\ C\ D\ E)$$

$$T \sim (B\ C)\ (D\ E)$$

e però le 60 rotazioni producono sui cinque sistemi le 60 sostituzioni del gruppo alterno.

Invece dei cinque sistemi di spigoli possiamo considerare come elementi cinque ottaedri regolari inscritti nell' icosaedro, poichè i sei punti medii degli spigoli di un sistema sono appunto i vertici di un ottaedro regolare. Le rotazioni del gruppo icosaedrale che lasciano fermo un ottaedro formano un gruppo tetraedrale entro il quale abbiamo un gruppo diedrale di 4 rotazioni *(Vierergruppe)* i cui tre assi sono le diagonali dell'ottaedro. Il gruppo icosaedrale contiene quindi 5 di questi sottogruppi del 4.° ordine che sono fra loro affini, come risulta anche dal teorema di Sylow.

§. 56. — Dalle nostre ricerche risulta che sarà possibile dare ai poliedri regolari tale orientazione entro la sfera complessa che le rotazioni del loro gruppo, tradotte in sostituzioni lineari secondo la formola (I) §. 51 di CAYLEY, diano luogo alle forme normali dei gruppi (§§. 46 – 49).

Pei gruppi ciclici si ottiene tale coincidenza inscrivendo la base della piramide regolare nel cerchio equatoriale e situando quindi il vertice in $z = 0$, ovvero in $z = \infty$.

Pei gruppi del secondo tipo basta situare i due vertici della doppia piramide in $z = 0$, $z = \infty$ ed inoltre un vertice della base in $z = i$.

Il gruppo del tetraedro essendo contenuto come sottogruppo (invariante) in quello dell'ottaedro, basterà occuparsi di quest'ultimo. Otteniamo la forma normale *d*) §. 48 per questo gruppo semplicemente col far coincidere le tre diagonali dell'ottaedro coi tre assi coordinati, onde due dei vertici saranno in $z = 0$, $z = \infty$ e gli altri quattro sul cerchio equatoriale in

$$z = \pm 1 \,, \; z = \pm i \,.$$

Allora le sostituzioni $z' = i^{\varepsilon} z$ sono le rotazioni attorno al diametro $\overline{0\infty}$, le sostituzioni

$$z' = \frac{i^{\varepsilon}}{z}$$

corrispondono ai ribaltamenti attorno agli 0ξ, 0η ed alle loro bisettrici e le rimanenti sono rotazioni di $\frac{2\pi}{3}$, nel senso positivo o negativo, attorno alle congiungenti i centri di due facce parallele opposte.

Per l'icosaedro situiamolo in primo luogo in guisa che due vertici opposti siano in

$$z = 0, \; z = \infty$$

e la rotazione S di ampiezza $= \frac{2\pi}{5}$ attorno al diametro $\overline{0\infty}$ sarà data da

$$\text{S)} \quad z' = \varepsilon z \quad \left(\varepsilon = e^{\frac{2\pi i}{5}}\right).$$

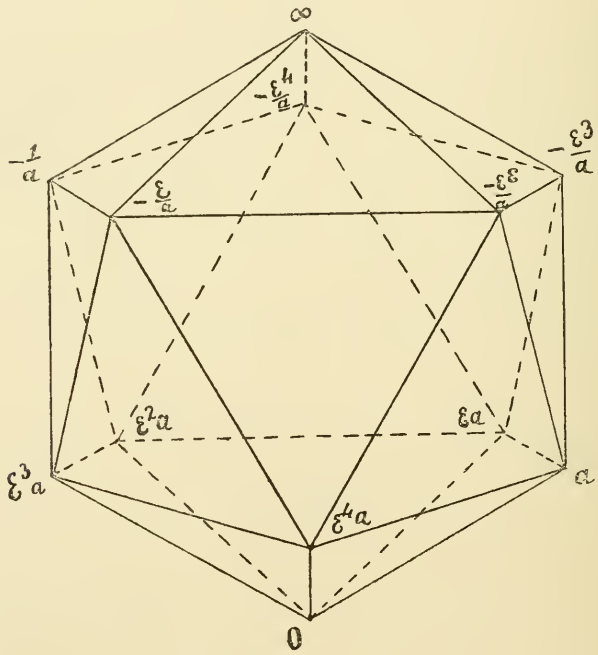
Orientiamo inoltre l'icosaedro in guisa che uno dei cinque vertici circostanti a $z = 0$ si disponga sul piano $\xi\,\zeta$ dalla parte delle ξ positive.

Se indichiamo con a il valore della variabile complessa in questo vertice sarà a reale, positiva e > 1. I cinque vertici circostanti $z = 0$ saranno

$$z = a,\ \varepsilon a,\ \varepsilon^2 a,\ \varepsilon^3 a,\ \varepsilon^4 a$$

e i cinque opposti saranno (V. fig. 2.ª)

Fig. 2.



$$z = -\frac{1}{a}\ ,\quad -\frac{\varepsilon}{a}\ ,\quad -\frac{\varepsilon^2}{a}\ ,\quad -\frac{\varepsilon^3}{a}\ ,\quad -\frac{\varepsilon^4}{a}\ .$$

Se consideriamo la rotazione T a periodo 2 attorno alla congiungente i punti medii dei due spigoli opposti $\overline{(0, a)}$, $\overline{\left(\infty, -\frac{1}{a}\right)}$ essa avrà per espressione analitica

$$z' = \frac{a - z}{a z + 1}$$

e poichè d'altronde deve scambiare εa con $\varepsilon^4 a$ avremo

$$\varepsilon^4 = \frac{1 - \varepsilon}{\varepsilon a^2 + 1}$$

onde

$$a^2 = 1 - \varepsilon - \varepsilon^4 = (\varepsilon + \varepsilon^4)^2$$

e però, essendo $\varepsilon + \varepsilon^4 = 2 \cos \frac{2\pi}{5}$ positivo:

$$a = \varepsilon + \varepsilon^4.$$

La T ha dunque l'espressione

$$\text{T)}\ z' = \frac{\varepsilon + \varepsilon^4 - z}{(\varepsilon + \varepsilon^4)\, z + 1} = \frac{(\varepsilon^4 - \varepsilon)\, z + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3)\, z - (\varepsilon^4 - \varepsilon)}.$$

Le sostituzioni superiori S, T sono appunto quelle che al §. 49 abbiamo costruito come generatrici del gruppo dell'icosaedro sotto forma normale.

§. 57. — Trattiamo ora rapidamente il problema di determinare *i gruppi finiti di movimenti di 1.ª e 2.ª specie della sfera in se stessa.*

Un tale gruppo G contiene necessariamente tanti movimenti di 1.ª quanti di 2.ª specie e quelli di 1.ª specie formano in G un sottogruppo invariante Γ d'indice 2; Γ appartiene quindi ad uno dei cinque tipi di gruppi dei poliedri regolari.

Per trovare dunque tutti questi gruppi basta esaminare ciascun gruppo poliedrale Γ e *ampliarlo* con un movimento t di 2.ª specie, che trasformi Γ in se stesso e tale che t^2 sia in Γ: allora sarà

$$G = (\Gamma, t\Gamma)$$

uno dei gruppi richiesti.

Limitiamoci qui ai casi che più ci interessano al nostro scopo e cioè all'ampliamento dei gruppi dell'ottaedro e dell'icosaedro, avvertendo che, mediante considerazioni perfettamente analoghe, si può esaurire la ricerca per gli altri gruppi.

Un movimento t di 2.ª specie, che trasformi il gruppo ottaedrale od icosaedrale in se medesimo, deve trasformare le rotazioni a periodo 4 dell'ottaedro o quelle a periodo 5 dell'icosaedro in rotazioni della medesima specie, appartenenti al gruppo, e poichè i poli di queste rotazioni sono unicamente i vertici del poliedro, dovrà la t trasformare il poliedro

in se medesimo [1]). Ora, associando a t una sostituzione γ del gruppo, possiamo far sì che il movimento equivalente di 2.ª specie

$$t' = t\gamma$$

porti un vertice nell'opposto e quindi tutti gli altri vertici negli opposti. Questo movimento t' non sarà quindi altro che l'inversione (§. 52)

$$z' = -\frac{1}{z_0}.$$

Così otteniamo, tanto nel caso dell'ottaedro che in quello dell'icosaedro, un solo ampliamento possibile. Quante riflessioni contiene il gruppo ampliato? Per vederlo, si osservi che l'inversione t' è a periodo 2 ed è permutabile con qualunque movimento. Un movimento di 2.ª specie $t'\gamma$ sarà quindi a periodo 2 quando lo sia γ ed inversamente, se γ è un ribaltamento, la $t'\gamma$ è evidentemente la riflessione sul cerchio massimo il cui piano è normale all'asse di ribaltamento. Così adunque nel gruppo ampliato dell'ottaedro avremo *nove* riflessioni e in quello dell'icosaedro *quindici;* i piani di queste riflessioni sono i piani di simmetria dell'ottaedro o dell'icosaedro.

I corrispondenti circoli di riflessione dividono la sfera rispettivamente in 48 e 120 triangoli sferici alternatamente simmetrici e congruenti con angoli di

$$\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{4}$$

nel caso dell'ottaedro e con angoli di

$$\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{5},$$

nel caso dell'icosaedro.

Si ottiene uno di questi triangoli congiungendo con archi di circolo massimo i tre vertici di una faccia del poliedro e suddividendo poi questo triangolo equilatero in *sei* triangoli minori per mezzo delle tre altezze sferiche. Queste reti di 48 o 120 triangoli simmetrici o congruenti in

---

[1]) Pel tetraedro invece bisogna aver riguardo all'altra possibilità che il tetraedro venga trasformato nell'opposto (coi vertici opposti) onde due possibili ampliamenti.

cui la sfera risulta divisa diconsi la *rete ottaedrica* o *la rete icosaedrica.* I movimenti del gruppo ampliato sono tutti e soli i 48 o 120 movimenti di (1.ª e 2.ª specie) che riportano la rete in se medesima. Uno qualunque di questi triangoli può assumersi come *campo fondamentale* del gruppo, nel senso che ogni punto della sfera può trasportarsi con una sostituzione del gruppo nel triangolo fondamentale, mentre da un punto ad un altro del triangolo fondamentale non si può passare con una sostituzione del gruppo. Dicendo *equivalenti* rispetto al gruppo due punti z, z', della sfera quando z' è legata a z da una sostituzione del gruppo, possiamo enunciare il risultato finale così:

Ogni punto della sfera è equivalente ad uno e ad un solo punto del triangolo fondamentale.

PARTE SECONDA

Teoria delle equazioni algebriche secondo Galois

Capitolo V.

Irriducibilità delle equazioni. — Risolvente di Galois. — Gruppo di Galois per un'equazione e sue proprietà fondamentali. — Formazione generale delle risolventi e loro gruppo. — Equazioni composte e loro riduzione a successive equazioni semplici.

§. 58. — Prima di studiare le applicazioni della teoria dei gruppi alle questioni che concernono la risoluzione delle equazioni algebriche, conviene ritornare sopra alcuni concetti fondamentali dell'algebra per bene precisarne il senso.

Una funzione razionale intera

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

di una variabile x dicesi *irriducibile* quando è impossibile scindere $f(x)$ nel prodotto di fattori di grado minore, i cui coefficienti siano *razionalmente noti*. Questo concetto d'*irriducibilità* non ha senso preciso se non quando venga fissato quali sono le quantità che, in una data questione, si considerano come razionalmente note, se non quando si fissi cioè, come diremo con Kronecker [1]), il *campo di razionalità*. Per definire il campo di razionalità basterà dare quelle quantità fondamentali

$$R, R', R'' \ldots$$

del campo stesso, per le quali tutte le altre, che si considerano come

---

[1]) Kronecker. — *Grundzüge einer arithmetischen Theorie der algebraischen Grössen.*

note, sono nel senso ordinario razionalmente esprimibili; allora il campo di razionalità, che indicheremo colla notazione di KRONECKER

$$(R, R', R'' \ldots)$$

conterrà tutte e sole quelle quantità che sono funzioni razionali a coefficenti interi di R, R', R''...

Così formano un campo di razionalità gli ordinarii numeri razionali, e questo campo è evidentemente contenuto in qualsiasi altro campo di razionalità; esso si dirà perciò il campo *assoluto* di razionalità e si denoterà col simbolo [1]. Così pure formano un campo di razionalità tutti i numeri della forma

$$a + b\sqrt{5},$$

essendo a, b frazioni ordinarie; qui si ha una sola quantità fondamentale nel campo e cioè $R = \sqrt{5}$.

Quando parliamo della irriducibilità o della riducibilità di una funzione razionale intera $f(x)$, intendiamo naturalmente che i coefficienti di $f(x)$ debbono essere dati, cioè appartenenti al campo di razionalità e, in generale, ove non si avverta il contrario, s'intenderà che il campo di razionalità del quale si parla sia quello determinato dai coefficienti di $f(x)$. Altrimenti bisognerà parlare della irriducibilità o riducibilità della $f(x)$ in un determinato campo di razionalità $(R, R' R'' \ldots)$.

Se in particolari ricerche converrà considerare come note quantità che prima non si riguardavano come tali, si dirà che tali quantità *si aggiungono* al campo di razionalità e le quantità stesse si diranno *aggiunte*. Ad ogni *aggiunta* di nuove quantità il campo di razionalità si amplia e naturalmente può darsi che una funzione $f(x)$, irriducibile nel campo primitivo, diventi riducibile nel campo ampliato. Così p. e. $f(x) = x^2 - 7$, che è irriducibile nel campo assoluto di razionalità, diventa riducibile se si aggiunge $\sqrt{7}$ e si spezza nei due fattori lineari:

$$f(x) = (x - \sqrt{7})\,(x + \sqrt{7}).$$

Precisato così il concetto d'irriducibilità per le funzioni intere razionali di una variabile [1]), diremo che *l'equazione*

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$$

---

[1]) Considerazioni analoghe valgono per le funzioni razionali intere di più variabili.

è irriducibile in un determinato campo di razionalità (R, R', R''...), *se tale è la funzione* $f(x)$.

Ciò premesso, ricordiamo alcuni teoremi fondamentali, ai quali continuamente dovremo ricorrere nel seguito:

1.° *Se un'equazione* $F(x) = 0$ *ammette una radice della equazione irriducibile* $f(x) = 0$, *le ammette tutte.*

E infatti si determini il massimo comun divisore $\psi(x)$ di $F(x)$ e $f(x)$, ciò che si fa con processi *razionali*, sicchè i coefficienti di $\psi(x)$ apparterranno all'attuale campo di razionalità. Se $\psi(x)$ fosse di grado minore di $f(x)$, la $f(x)$, che ammette $\psi(x)$ come fattore, sarebbe riducibile.

Da questo teorema ne seguono due altri importanti:

2.° *Un'equazione irriducibile non può avere radici comuni con un'equazione di grado inferiore.*

3.° *Ogni funzione riducibile si può scindere in un solo modo in un prodotto di funzioni irriducibili.*

§. 59 – Sarà utile che, almeno nel caso speciale del campo assoluto di razionalità, dimostriamo la effettiva esistenza di funzioni irriducibili e diamo un procedimento che permetta di riconoscere se una funzione $f(x)$ *data* è riducibile o irriducibile.

Una funzione razionale $f(x)$ nel campo assoluto [1] di razionalità ha per coefficienti numeri razionali e, moltiplicandola per un numero intero, si può ridurre a coefficienti interi. Sia

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

una tale funzione con coefficienti a interi. Se δ è il massimo comun divisore dei coefficienti a, si dirà che δ è *il divisore della funzione* $f(x)$ [1]) e la funzione stessa si dirà *primitiva* se $\delta = 1$.

Cominciamo dal dimostrare il teorema di Gauss:

Se le funzioni $f(x)$, $\varphi(x)$ *razionali intere a coefficienti interi sono primitive, anche il loro prodotto* $f(x) . \varphi(x)$ *sarà una funzione della medesima specie.*

---

[1]) Con ciò si vuol significare che tutti i valori (interi) $f(m)$ che assume $f(x)$ per valori interi m di x, ammettono il divisore δ.

Poniamo

$$f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m$$
$$\varphi(x) = b_0 x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n$$
$$f(x).\varphi(x) = c_0 x^{m+n} + c_1 x^{m+n-1} + \ldots + c_{m+n-1} x + c_{m+n};$$

avremo

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

e in generale

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0,$$

coll'avvertenza che le a con indice superiore a m, come le b con indice superiore a n sono da farsi $= 0$. Se la $f(x) . \varphi(x)$ non fosse primitiva, esisterebbe almeno un fattore primo p comune a tutti i numeri c; ma siccome p non può dividere nè tutte le a nè tutte le b, poichè $f(x)$, $\varphi(x)$ sono primitive, supponiamo che sia a_r il coefficiente a con indice più *basso* non divisibile per p e così b_s il primo dei coefficienti b nella serie

$$b_0,\ b_1,\ b_2 \ldots$$

non divisibile per p. Avremo

$$r \leq m,\ s \leq n$$

e potrà anche darsi che uno dei due indici r, s sia $= 0$, ma non tutti due poichè p divide $c_0 = a_0 b_0$. Ora se consideriamo il coefficiente

$$c_{r+s} = \sum_{i=0}^{i=r+s} a_i b_{r+s-i},$$

vediamo che nel secondo membro tutti i termini, salvo $a_r b_s$, sono divisibili per p e quindi c_{r+s} non è divisibile per p contro l'ipotesi.

Dal teorema precedente segue il corollario:

Se le funzioni intere a coefficienti interi $f(x)$, $\varphi(x)$ hanno i rispettivi divisori α, β, sarà $\alpha\beta$ il divisore del prodotto $f(x) . \varphi(x)$.

Si ha infatti

$$f(x) = \alpha f_1(x),\ \varphi(x) = \beta \varphi_1(x),$$

dove $f_1(x)$, $\varphi_1(x)$ sono primitive e però anche il loro prodotto $f_1(x).\varphi_1(x)$, onde $f(x).\varphi(x) = \alpha\beta.f_1(x).\varphi_1(x)$ ha per divisore $\alpha\beta$.

Dimostriamo ora il teorema:

Se una funzione F (x), *a coefficienti interi, è riducibile essa potrà scindersi nel prodotto di due altre funzioni a coefficienti interi.*

Basterà evidentemente stabilire la proposizione nel caso che F (x) sia primitiva. Supponiamo che si abbia

$$F(x) = f(x) \,.\, \varphi(x)$$

avendo f, φ coefficienti razionali. Potremo moltiplicare per un conveniente intero N per modo che sia

$$N\,F(x) = f_1(x) \,.\, \varphi_1(x)\,,$$

essendo f_1, φ_1 a coefficienti interi. Se diciamo α, β i loro rispettivi divisori, sarà $\alpha\beta$ il divisore di N F (x) e, poichè F (x) è primitiva, avremo $N = \alpha\beta$, quindi otterremo

$$F(x) = \frac{f_1(x)}{\alpha} \,.\, \frac{\varphi_1(x)}{\beta}\,,$$

che è la decomposizione richiesta per F (x).

§. 60. — Dalle considerazioni superiori facilmente si trae la dimostrazione del teorema seguente, che ci assicura dell'esistenza di una classe assai estesa di funzioni irriducibili il cui grado è un numero n qualunque:

La funzione intera a coefficienti interi

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

è certamente irriducibile se un fattore primo p, che divide tutti i coefficienti

$$a_1, a_2, \ldots a_n\,,$$

non divide il primo a_0 ed a_n non è divisibile per p^2.

Supponiamo al contrario $f(x)$ riducibile; pei teoremi al §. 59 sarà decomponibile nel prodotto di due funzioni a coefficienti interi

$$\varphi(x) = \alpha_0 x^r + \alpha_1 x^{r-1} + \ldots + \alpha_{r-1} x + \alpha_r$$
$$\psi(x) = \beta_0 x^s + \beta_1 x^{s-1} + \ldots + \beta_{s-1} x + \beta_s\,.$$

Avremo $r+s=n$ e $a_n=\alpha_r\beta_s$, onde, per le ipotesi fatte, p dividerà uno ed uno solo dei due numeri α_r, β_s, poniamo β_s. Ora non potendo p dividere tutte le β, poichè altrimenti entrerebbe anche in $a_0=\alpha_0\beta_0$, sia β_k il coefficiente β, col massimo indice, non divisibile per p; sarà $0 \leq k < s$. Il coefficiente a_{r+k} di x^{s-k} in $f(x)$ sarà dato da

$$a_{r+k}=\alpha_r\,\beta_k+\alpha_{r-1}\,\beta_{k+1}+\alpha_{r-2}\,\beta_{k+2}+\ldots$$

e poichè tutti i termini della somma del 2.° membro sono divisibili per p, tranne il primo, sarebbe a_{r+k} con indice $r+k>0$ non divisibile per p, contro l'ipotesi. Vediamo ora come data una funzione $f(x)$ a coefficienti interi si possa, con un numero finito di tentativi, riconoscere se essa è riducibile od irriducibile. Serve a questo scopo un procedimento dato da Kronecker nell'opera citata. In primo luogo si osservi che, se m è il grado di $f(x)$, basterà limitarsi a ricercare gli eventuali divisori razionali di $f(x)$ di grado $n \leq \frac{m}{2}$. Per ogni grado n assegnato scegliamo ad arbitrio $n+1$ numeri interi disuguali

$$r_0,\ r_1,\ r_2 \ldots r_n$$

e consideriamo le $n+1$ funzioni razionali di grado n

$$g_0(x)=\frac{(x-r_1)(x-r_2)\ldots(x-r_n)}{(r_0-r_1)(r_0-r_2)\ldots(r_0-r_n)},\ g_1(x)=\frac{(x-r_0)(x-r_2)\ldots(x-r_n)}{(r_1-r_0)(r_1-r_2)\ldots(r_1-r_n)},\ldots$$

$$g_n(x)=\frac{(x-r_0)(x-r_1)\ldots(x-r_{n-1})}{(r_n-r_0)(r_n-r_1)\ldots(r_n-r_{n-1})},$$

le quali sono costruite in guisa che per un valore qualunque i dell'indice da 0 a n sia

$$g_i(r_i)=1,\ g_i(r_k)=0 \text{ per } i \neq k.$$

Sia ora $\varphi(x)$ un divisore razionale di grado n, a coefficienti interi, di $f(x)$. Potremo esprimere $\varphi(x)$ come un aggregato lineare omogeneo delle $n+1$ funzioni $g_i(x)$ colla formola

$$(1)\qquad \varphi(x)=\varphi(r_0)\,g_0(x)+\varphi(r_1)\,g_1(x)+\ldots+\varphi(r_n)\,g_n(x),$$

poichè infatti i due polinomii di grado n dalle due parti, coincidendo per $n+1$ valori diversi

$$r_0,\ r_1,\ldots r_n$$

dell'argomento x, sono identici. Ora, se $f(x) = \varphi(x) . \psi(x)$, sarà $f(r_i) = \varphi(r_i) . \psi(r_i)$, onde il numero intero $\varphi(r_i)$ dovrà dividere $f(r_i)$. A ciascuno dei coefficienti $\varphi(r_i)$ nel 2.° membro della (1) non potremo dunque attribuire che un numero finito di valori e perciò, con un numero finito di tentativi, potremo accertarci dell'esistenza, o meno del supposto divisore $\varphi(x)$.

§. 61. — Dopo aver precisato, colle considerazioni dei §§. precedenti, le nozioni di campo di razionalità e di riducibilità o irriducibilità di un'equazione, passiamo ora alla ricerca fondamentale per le applicazioni della teoria dei gruppi che consiste nel costruire, per una data equazione $f(x) = 0$, la così detta *risolvente di* Galois.

Sia

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0.$$

una equazione, *che noi supporremo sempre nel seguito priva di radici multiple* [1]), e indichiamo con

$$x_1, x_2, \ldots x_n$$

le sue radici. Consideriamo una funzione razionale (che potremo senz'altro supporre intera) delle radici, sia

$$V = \varphi(x_1, x_2, \ldots x_n).$$

Permutando entro φ le n radici nei $\pi(n)$ modi possibili, la V acquisterà $\pi(n)$ valori e si tratta in primo luogo di vedere come, scegliendo opportunamente la funzione φ, questi $\pi(n)$ valori possano supporsi non solo *algebricamente* ma anche *numericamente* distinti. Prendiamo per ciò semplicemente

$$V = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

colle costanti α tutte disuguali; i $\pi(n)$ valori di V sono certo allora *algebricamente* distinti, quando cioè si riguardino $x_1, x_2 \ldots x_n$ come variabili indipendenti. Ma poichè qui $x_1, x_2 \ldots x_n$ hanno valori numerici fissi, potrà ben darsi che fra questi valori ve ne siano di quelli *nume-*

---

[1]) È ben noto come alla risoluzione di un'equazione con radici multiple possa sostituirsi, con processi razionali, la risoluzione di altrettante equazioni a radici semplici.

ricamente eguali. Tuttavia potremo sempre evitare che ciò accada procedendo nel modo seguente:

Particolarizziamo ancora le α, ponendo

$$\alpha_1 = 1\,,\ \alpha_2 = h\,,\ \alpha_3 = h^2, \ldots \alpha_n = h^{n-1};$$

l'eguaglianza numerica fra due valori algebricamente distinti della V porta ad una relazione della forma:

$$(2)\quad h^{n-1}(x_{i_n} - x_{\lambda_n}) + h^{n-2}(x_{i_{n-1}} - x_{\lambda_{n-1}}) + \ldots + h(x_{i_2} - x_{\lambda_2}) + (x_{i_1} - x_{\lambda_1}) = 0,$$

dove $(i_1\, i_2 \ldots i_n)$, $(\lambda_1\, \lambda_2 \ldots \lambda_n)$ indicano due diverse permutazioni degli indici $1, 2, 3 \ldots n$. Scelte le due permutazioni, la (2) è soddisfatta soltanto per $n-1$ valori di h (fra i quali possono anche esservene degli eguali); basta dunque evitare per h un numero finito di valori per essere sicuri che i $\pi(n)$ valori di V saranno numericamente distinti [1]).

Ciò premesso, indichiamo con

$$s_1 = 1,\ s_2, s_3 \ldots s_{\pi(n)}$$

le $\pi(n)$ sostituzioni sulle x e con V_{s_i} indichiamo il valore che assume la $V = V_{s_i}$, effettuandovi sulle x la sostituzione s_i. I $\pi(n)$ valori distinti della V saranno

$$(a)\qquad V_{s_1}\,,\ V_{s_2} \ldots V_{s_{\pi(n)}}$$

e inversamente a ciascuno di questi valori corrisponderà una sostituzione perfettamente determinata. Ora, indicando con Y una variabile, si costruisca il polinomio di grado $\pi(n)$ in Y:

$$(b)\qquad \psi(Y) = (Y - V_{s_1})(Y - V_{s_2}) \ldots (Y - V_{\pi(n)});$$

i suoi coefficienti sono le funzioni simmetriche elementari dei $\pi(n)$ valori V e quindi, come è chiaro, saranno funzioni simmetriche delle radici della proposta ed esprimibili per ciò razionalmente pei coefficienti di questa. Avremo dunque

$$\psi(Y) = Y^{\pi(n)} + \beta_1 Y^{\pi(n)-1} + \beta_2 Y^{\pi(n)-2} + \ldots + \beta_{\pi(n)}\,,$$

i coefficienti β essendo razionalmente noti. L'equazione $\psi(Y) = 0$, che ha

---

[1]) In qual modo possano in pratica escludersi questi valori di h si vedrà ora subito.

manifestamente per radici le $\pi(n)$ quantità distinte (a), dicesi *risolvente di* GALOIS della equazione data.

Se nel costruire la risolvente di GALOIS, p. e. colla funzione

$$V = x_1 + hx_2 + \ldots + h^{n-1} x_n,$$

si lascia h indeterminata, indi si eguaglia a zero il discriminante di $\psi(Y) = 0$, si otterrà per h una equazione le cui radici sono i valori di h da evitarsi.

§. 62. — La risolvente di GALOIS gode di importanti proprietà, delle quali la fondamentale è data dal teorema seguente:

Qualunque funzione razionale

$$F(x_1 x_2 \ldots x_n)$$

delle radici della proposta è razionalmente esprimibile per una qualunque radice della risolvente di GALOIS, *p. e. per* $V_{s_1} = V_1$.

Denotiamo ancora con

$$F_{s_1},\ F_{s_2}, \ldots F_{s_{\pi(n)}} \tag{3}$$

i valori che assume $F(x_1, x_2, \ldots x_n)$ effettuando sulle x le $\pi(n)$ sostituzioni, avvertendo però che non supponiamo affatto che i $\pi(n)$ valori (3) siano tutti numericamente distinti. Avendo $\psi(Y)$ il significato dato dalla (b), consideriamo la funzione razionale intera $\Phi(Y)$ di grado $\pi(n) - 1$ in Y data dalla formola

$$\Phi(Y) = \left\{ \frac{F_{s_1}}{Y - V_{s_1}} + \frac{F_{s_2}}{Y - V_{s_2}} + \ldots + \frac{F_{s_{\pi(n)}}}{Y - V_{s_{\pi(n)}}} \right\} . \psi(Y); \tag{4}$$

i coefficienti di $\Phi(Y)$ sono funzioni simmetriche di $x_1, x_2 \ldots x_n$ e perciò razionalmente noti. Facendo nella (4) $Y = V_{s_i}$, otteniamo

$$\Phi(V_{s_i}) = F_{s_i} . \psi'(V_{s_i}),$$

indicando con $\psi'(Y)$ il polinomio derivato di $\psi(Y)$. Siccome $\psi(Y) = 0$ non ha radici multiple si ha $\psi'(V_{s_i}) \neq 0$, indi

$$F_{s_i} = \frac{\Phi(V_{s_i})}{\psi'(V_{s_i})},$$

formola che vale per una qualunque s_i.

Servendosi ora della relazione

$$\psi(V_{s_i}) = 0$$

cui soddisfa V_{s_i}, è ben noto come la funzione razionale fratta $\frac{\Phi(V_{s_i})}{\psi'(V_{s_i})}$, possa porsi sotto la forma di una funzione razionale intera $\Theta(V_{s_i})$ di grado $\pi(n) - 1$ al massimo in V_{s_i} ed affatto indipendente dall'indice i. Avremo dunque

$$(c) \qquad F_{s_i} = \Theta(V_{s_i})$$

ed in particolare

$$F_{s_1} = F(x_1\, x_2 \ldots x_n) = \Theta(V_{s_1}),$$

ciò che dimostra il teorema enunciato. Ma abbiamo conseguito insieme anche l'altro risultato d'importanza fondamentale:

Nella relazione

$$F(x_1\, x_2 \ldots x_n) = \Theta(V_{s_1}),$$

che lega una funzione razionale qualunque delle radici della proposta razionalmente ad una radice V_{s_1} *della risolvente di* Galois, *è lecito fare qualunque sostituzione sulle* x, *senza che la relazione cessi di essere verificata.*

§. 63. — La proprietà fondamentale sopra dimostrata dà luogo a varie conseguenze che importa notare. In primo luogo, prendendo per $F(x_1\, x_2 \ldots x_n)$ una qualunque delle radici della proposta, vediamo che:

Ogni radice della proposta è razionalmente esprimibile per una radice arbitraria della risolvente di Galois.

Basterebbe dunque conoscere *una* radice della risolvente di Galois per ottenere la risoluzione completa della proposta.

Prendasi ora per $F(x_1\, x_2 \ldots x_n)$ una qualunque delle altre radici della risolvente stessa di Galois e si avrà il teorema:

La risolvente di Galois *gode della proprietà che tutte le sue radici possono esprimersi razionalmente per una qualunque di esse.*

Ogni equazione (a radici diseguali) che goda della proprietà qui rilevata per la risolvente di Galois dicesi un'equazione *normale*, sicchè: *ogni risolvente di* Galois *è un'equazione normale.*

Si osservi poi che se

$$\psi(Y) = 0, \quad \bar{\psi}(Y) = 0$$

sono due diverse risolventi di GALOIS per una medesima equazione, costruite con due diverse funzioni fondamentali

$$V(x_1 x_2 \ldots x_n), \; \bar{V}(x_1 x_2 \ldots x_n),$$

si avrà pel teorema fondamentale:

$$\bar{V}_{s_i} = \Theta(V_{s_i}),$$

essendo Θ razionale intera, cioè: *Due diversi risolventi di* GALOIS *della proposta si ottengono l'una dall'altra con una trasformazione di* TSCHIRNHAUS. Noi riguarderemo come non essenzialmente distinte due tali equazioni e parleremo per ciò *della risolvente* di GALOIS, intendendo di assumerla sotto una qualunque delle infinite forme equivalenti.

La risolvente di GALOIS, che è certamente priva di radici multiple, può essere riducibile o irriducibile. In particolare essa può essere riducibile, sia nel campo di razionalità determinato dai coefficienti della primitiva, sia perchè, coll'aggiunta di nuove quantità, il campo stesso è stato ampliato. In ogni caso però dimostreremo che i fattori irriducibili, in cui viene a scindersi il primo membro $\psi(Y)$ della risolvente, sono tutti di egual grado. Sebbene questa proprietà risulti anche indirettamente dai teoremi dei §§. seguenti, non sarà inutile darne una dimostrazione diretta, provando che essa sussiste analogamente per tutte le equazioni normali. Dimostriamo cioè il teorema:

Ogni equazione normale riducibile si scinde in fattori irriducibili tutti di egual grado

Sia

$$f(x) = 0$$

un'equazione normale (priva di radici multiple) di grado n e riducibile. Basterà evidentemente dimostrare che se

$$\varphi(x) = (x - x_1)(x - x_2) \ldots (x - x_r)$$

è un fattore irriducibile di $f(x)$ di grado r, nessun altro fattore irriducibile di $f(x)$ potrà avere un grado maggiore di r. Sia $\varphi_1(x)$ un altro fattore irriducibile di $f(x)$ e sia x_i una sua radice; essendo $f(x) = 0$ un'equazione normale, avremo

$$x_i = \Theta(x_1)$$

con Θ razionale intera in x_1. Ora, avendosi

$$\varphi_1(x_i) = \varphi_1(\Theta(x_1)) = 0\,,$$

vediamo che l'equazione

$$\varphi_1(\Theta(x)) = 0$$

ammette la radice x_1 dell'equazione irriducibile $\varphi(x) = 0$ e però ammette tutte le altre $x_2, x_3 \ldots x_r$, cioè si ha:

$$\varphi_1(\Theta(x_1)) = 0\,,\ \varphi_1(\Theta(x_2)) = 0 \ldots \varphi_1(\Theta(x_r)) = 0\,,$$

ossia le espressioni

$$\Theta(x_1)\,,\ \Theta(x_2)\,,\ \ldots\ \Theta(x_r)$$

sono altrettante radici di $\varphi_1(x) = 0$. D'altronde il polinomio di grado r in x:

$$(x - \Theta(x_1))\ (x - \Theta(x_2)) \ldots (x - \Theta(x_r))\,,$$

che è un fattore di $\varphi_1(x)$, ha i coefficienti funzioni simmetriche di $x_1\, x_2 \ldots x_r$ e per ciò razionalmente esprimibili pei coefficienti di $\varphi(x)$, cioè razionalmente noti. È quindi impossibile che il grado di $\varphi_1(x)$ sia maggiore di r.

§. 64. — Veniamo ora alle considerazioni che legano la teoria delle equazioni colla teoria dei gruppi, alla nozione fondamentale del *gruppo di* Galois per una data equazione.

Consideriamo un fattore *irriducibile* $\varphi(Y)$ del 1.° membro $\psi(Y)$ della risolvente di Galois e siano

$$(d) \qquad V_{s_1}\,,\ V_{s_2} \ldots V_{s_r}$$

le r radici di $\varphi(Y)$. Dimostriamo il teorema:

Le r sostituzioni sulle radici della proposta

$$(c) \qquad s_1\, s_2\, s_3 \ldots s_r\,,$$

colle quali si passa dalla prima alle altre radici del fattore irriducibile $\varphi(Y)$ della risolvente di Galois, *formano un gruppo.*

Tanto risulta facilmente dalle proprietà dimostrate al §. 62. Essendo V_{s_i} una qualunque delle r radici (d) di $\varphi(Y)$, si ha

$$(5) \qquad V_{s_i} = \Theta(V_{s_1})\,,$$

ove Θ è razionale intera in V_{s_1}. Per il teorema alla fine del §. 62, pos-

siamo nella (5) permutare in qualsivoglia modo le x e la relazione rimane ancora soddisfatta.

Operando una qualunque s_k delle sostituzioni (e), avremo quindi

$$V_{s_i s_k} = \Theta (V_{s_k}). \tag{6}$$

Ora, essendo

$$\varphi (V_{s_i}) = \varphi [\Theta (V_{s_1})] = 0,$$

la equazione $\varphi (\Theta (Y)) = 0$, che ammette la radice V_{s_1} dell'equazione irriducibile $\varphi (Y) = 0$, le ammette tutte e si ha in particolare

$$\varphi (\Theta (V_{s_k})) = 0$$

cioè, per la (6)

$$\varphi (V_{s_i s_k}) = 0.$$

Dunque $V_{s_i s_k}$ è una radice della $\varphi (Y) = 0$, cioè

$$V_{s_i s_k} = V_{s_l},$$

essendo l un indice da 1 a r. Ne segue

$$s_i s_k = s_l,$$

formola che ci prova appunto che le r sostituzioni

$$s_1, \; s_2, \ldots s_r$$

formano un gruppo c. d. d. Indicando questo gruppo con G_r, distribuiamo le $\pi (n)$ sostituzioni del gruppo totale rispetto al sottogruppo

$$G_r = (s_1, \; s_2 \ldots s_r)$$

nel solito quadro

$$G_{\pi(n)} = \left\{ \begin{array}{l} s_1, \; s_2 \ldots s_r \\ g_2 s_1, \; g_2 s_2 \ldots g_2 s_r \\ \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \\ g_q s_1, \; g_q s_2 \ldots g_q s_r \end{array} \right. \qquad \left(q = \frac{\pi (n)}{r} \right).$$

Mediante considerazioni affatto analoghe a quelle del §. precedente, vediamo subito che le radici V della risolvente di Galois, i cui indici sono le sostituzioni di una medesima orizzontale nel quadro superiore,

appartengono ad un medesimo fattore irriducibile della risolvente. Sia infatti p. e. $\varphi_1(Y)$ il fattore irriducibile cui appartiene V_{g_2}; avremo

$$V_{g_2} = \Theta(V_{s_1}),$$

essendo Θ razionale intera nell'argomento V_{s_1}. Eseguendo in questa relazione la sostituzione s_i, come è lecito (§. 62), ne deduciamo

$$V_{g_2 s_i} = \Theta(V_{s_i}).$$

Ma si ha $\varphi_1(V_{g_2}) = \varphi_1(\Theta(V_{s_1})) = 0$. onde si trae, nel solito modo,

$$\varphi_1(\Theta(V_{s_i})) = \varphi_1(V_{g_2 s_i}) = 0;$$

dunque tutte le radici $V_{g_2 s_i}$ della seconda orizzontale appartengono ad un medesimo fattore irriducibile.

Vediamo così che da qualunque fattore irriducibile della risolvente di Galois si parta, le sostituzioni sulle x, che fanno passare dall'una all'altra delle sue radici, formano sempre il medesimo gruppo G_r. Questo dicesi il *gruppo di* Galois per l'equazione proposta.

Osserviamo poi che, essendo ciascuna delle n radici della proposta funzione razionale intera di V_{s_1}, potremo scrivere

$$x_1 = \Theta_1(V_{s_1}), x_2 = \Theta_2(V_{s_1}) \ldots (x_n = \Theta_n(V_{s_1})$$

e per il teorema al §. 62, potremo eseguire in questa relazione una qualunque sostituzione sulle x, in particolare una sostituzione del gruppo di Galois, sicchè

$$\Theta_1(V_{s_i}) . \Theta_2(V_{s_i}), \ldots \Theta_n(V_{s_i})$$

saranno le radici stesse $x_1, x_2 \ldots x_n$ permutate secondo la sostituzione s_i. Possiamo quindi anche definire il gruppo di Galois nel modo seguente:

Si esprimano le n radici x della proposta razionalmente per una radice della risolvente di Galois; *cangiando in queste espressioni quella radice in tutte le altre appartenenti al medesimo fattore irriducibile della risolvente, le n radici x si permutano fra loro appunto secondo le sostituzioni del gruppo di* Galois.

§. 65. — Stabilita nel §. precedente l'*esistenza* del gruppo di Galois, andiamo ora ad occuparci delle sue proprietà caratteristiche, che vengono espresse nei tre seguenti teoremi fondamentali.

I). *Se una funzione razionale* F $(x_1, x_2 \ldots x_n)$ *delle n radici di* $f(x) = 0$ *rimane* **numericamente** *invariata per qualsiasi sostituzione del gruppo* di GALOIS, *essa è razionalmente nota, cioè appartiene al campo attuale di razionalità.*

Indicando con F_{s_i} il valore che assume F $(x_1, x_2, \ldots x_n)$ dopo eseguita sulle x la sostituzione s_i del gruppo di GALOIS, si ha per ipotesi

$$F_{s_1} = F_{s_2} = F_{s_3} = \ldots = F_{s_r} .$$

D'altronde abbiamo (§. 62)

$$F_{s_i} = \Theta (V_{s_i}) ,$$

essendo Θ una funzione razionale (intera) del suo argomento. Per ciò il valore numerico di F $(x_1 x_2 \ldots x_n)$ può anche esprimersi con

$$F (x_1 x_2 \ldots x_n) = \frac{1}{r} \left\{ \Theta (V_{s_1}) + \Theta (V_{s_2}) + \ldots + \Theta (V_{s_r}) \right\} .$$

Ora il secondo membro, come funzione simmetrica delle radici del primo fattore irriducibile $\varphi (Y) = 0$ della risolvente di GALOIS, appartiene appunto al campo attuale di razionalità c. d. d.

II). *Inversamente, se una funzione razionale* F $(x_1, x_2 \ldots x_n)$ *delle radici di* $f(x) = 0$ *è razionalmente nota, essa non cangia di valore numerico, effettuando sulle* x *qualunque sostituzione del gruppo di* GALOIS.

Si abbia infatti

$$F (x_1, x_2 \ldots x_n) = A ,$$

essendo A una quantità del campo attuale di razionalità. Esprimendo F $(x_1 \ldots x_n)$ in funzione razionale intera di V_{s_1}, avremo

$$\Theta (V_{s_1}) - A = 0$$

e però l'equazione

$$\Theta (Y) - A = 0 ,$$

ammettendo la radice V_{s_1} del fattore irriducibile φ (Y), ammetterà anche tutte le altre e si avrà quindi

$$\Theta (V_{s_1}) = \Theta (V_{s_2}) = \ldots = \Theta (V_{s_r}) = A .$$

D'altronde si ha (§. 62) $F_{s_i} = \Theta(V_{s_i})$ onde, segue appunto

$$F_{s_1} = F_{s_2} = \ldots = F_{s_r},$$

come è enunciato nel teorema.

Come corollario di questo teorema, si ha che se due funzioni razionali delle radici $F(x_1 x_2 \ldots x_n)$, $\overline{F}(x_1 x_2 \ldots x_n)$ hanno il medesimo valore numerico

$$F(x_1 x_2 \ldots x_n) = \overline{F}(x_1 x_2 \ldots x_n),$$

si avrà anche per qualunque sostituzione s_i *del gruppo di* Galois:

$$F_{s_i} = \overline{F}_{s_i},$$

poichè $F(x_1 x_2 \ldots x_n) - \overline{F}(x_1 x_2 \ldots x_n)$ è razionalmente nota $= 0$. Ma non è invece lecito, in generale, concludere $F_U = \overline{F}_U$, se U non appartiene al gruppo di Galois.

Dimostriamo in fine come le proprietà superiormente stabilite pel gruppo di Galois siano caratteristiche per le sostituzioni di questo gruppo col teorema:

III). *Nessuna sostituzione fuori del gruppo di* Galois *può lasciare invariate tutte le funzioni razionali delle radici razionalmente note.*

Indicando con ρ un'indeterminata nel campo di razionalità, la funzione razionale delle radici

$$F = (\rho - V_{s_1})(\rho - V_{s_2}) \ldots (\rho - V_{s_r}) = \varphi(\rho)$$

è razionalmente nota; ma una sostituzione g fuori del gruppo di Galois la cangia in

$$F_g = (\rho - V_{s_1 g})(\rho - V_{s_2 g}) \ldots (\rho - V_{s_r g}),$$

che può coincidere numericamente col valore iniziale F solo per un numero finito di valori di ρ che possiamo sempre evitare (Cf. §. 61).

Le proprietà dimostrate caratterizzano il gruppo di Galois per una equazione come il complesso di tutte quelle sostituzioni sulle radici che, applicate a tutte le relazioni razionali esistenti fra le radici, le lasciano ancora sussistere. Risulta di qui che se, per una data equazione $f(x) = 0$, si riesce a trovare un gruppo Γ di sostituzioni sulle radici tale che ogni sostituzione di Γ lasci invariata numericamente qualunque funzione ra-

zionale delle radici razionalmente nota, il gruppo di GALOIS coinciderà con Γ o conterrà Γ come sottogruppo.

§. 66. — Il gruppo di GALOIS per un'equazione $f(x) = 0$ è essenzialmente dipendente dal campo attuale di razionalità (R, R', R'' ...).

Se il campo si amplia per *aggiunta* di nuove quantità può accadere naturalmente che varii il gruppo di GALOIS. In ogni caso sussiste il teorema: *Ampliando il campo di razionalità, il gruppo di* GALOIS *rimarrà lo stesso, ovvero si abbasserà ad un suo sottogruppo.*

E invero se il primitivo fattore irriducibile

$$\varphi(Y) = (Y - V_{s_1})(Y - V_{s_2}) \ldots (Y - V_{s_r})$$

della risolvente di GALOIS rimane irriducibile nel nuovo campo, il gruppo rimane evidentemente lo stesso. Se al contrario diventa riducibile, sia

$$\varphi_1(Y) = (Y - V_{s_1})(Y - V_{s_2}) \ldots (Y - V_{s_i})$$

un suo fattore irriducibile; sarà

$$\Gamma_i = (s_1, s_2, \ldots s_i)$$

il nuovo gruppo di GALOIS che è un sottogruppo del primitivo G_r.

Ciò premesso, osserviamo che se $F(x_1 x_2 \ldots x_r)$ è una funzione razionale qualunque delle radici della proposta $f(x) = 0$, sussiste il teorema:

Quelle sostituzioni del gruppo G_r *di* GALOIS *che lasciano* **numericamente** *invariata la* $F(x_1 x_2 \ldots x_r)$ *formano in* G_r *un sottogruppo* [1]).

Potrebbe sembrare a prima vista che il teorema dovesse valere per tutte le sostituzioni anche fuori del gruppo di GALOIS. Ciò sarebbe esatto se si trattasse d'invariabilità *algebrica;* ma non vale più per l'invariabilità *numerica* che può aver luogo senza la prima. Basti citare il seguente esempio:

L'equazione

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \ldots + x + 1 = 0, \text{ ove supponiamo } n > 5$$

ha le $n - 1$ radici $x_r = e^{\frac{2\pi i r}{n}}$ $(r = 1, 2, \ldots n - 1)$.

Ora il prodotto $x_1 x_{n-1} = 1$ è lasciato numericamente invariato dalle due sostituzioni

$$(x_1 x_2)(x_{n-1} x_{n-2})$$
$$(x_1 x_{n-1})(x_2 x_3);$$

ma il prodotto di queste due sostituzioni lo cangia in $x_3 x_{n-2}$ che non ha più il valore 1.

E infatti, se s_i, s_k sono due tali sostituzioni di G_r, si ha

$$F_{s_i} = F_{s_1}, \quad F_{s_k} = F_{s_1} \; (s_1 = 1)$$

e quindi, eseguendo sulla prima relazione la sostituzione s_k del gruppo di Galois come è lecito (§. 65), avremo

$$F_{s_i s_k} = F_{s_k} = F_{s_1},$$

cioè anche il prodotto $s_i s_k$ lascia F numericamente invariata c. d. d.

Dimostriamo ora il seguente teorema fondamentale:

Se si amplia il campo di razionalità aggiungendovi una funzione razionale $F(x_1 x_2 \ldots x_n)$ *delle radici, il gruppo* G_r *di* Galois *si abbasserà a quel suo sottogruppo* Γ, *le cui sostituzioni lasciano numericamente invariata la funzione* $F(x_1 x_2 \ldots x_n)$ *aggiunta.*

Che il nuovo gruppo contenga soltanto sostituzioni di Γ risulta evidente dall'osservare che, essendo

$$z_1 = F(x_1, x_2 \ldots x)$$

razionale nel nuovo campo, le sostituzioni del nuovo gruppo di Galois debbono lasciarla numericamente invariata. Per dimostrare poi che tutte le sostituzioni γ di Γ appartengono al nuovo gruppo di Galois basterà, pel teorema III, §. 65, mostrare che γ lascia invariata *qualunque* funzione razionale delle radici razionalmente nota. Una tale funzione $U(x_1 x_2 \ldots x_n)$, appartenendo al campo di razionalità $(R, R', R'' \ldots z_1)$ ampliato dal primitivo $(R, R', R'' \ldots)$ coll'aggiunta di z_1, sarà esprimibile razionalmente per z_1 colla formola

$$U_1 = U(x_1 x_2 \ldots x_n) = \Theta(z_1),$$

ove Θ è razionale in z_1 con coefficienti razionali nell'antico campo $(R, R', R''..)$. Ad una tale relazione è applicabile, per le proprietà fondamentali al §. precedente, qualunque sostituzione dell'antico gruppo di Galois, in particolare la γ; avremo quindi

$$U_\gamma = \Theta(z_\gamma)$$

e poichè, per ipotesi, $z_\gamma = z_1$ sarà anche

$$U_\gamma = U_1,$$

ciò che dimostra il teorema.

§. 67. — Vedremo in seguito come tutte le proprietà dei gruppi che abbiamo studiato nella prima parte del presente corso si traducano, colla nozione del gruppo di GALOIS per un'equazione, in altrettante proprietà dell'equazione stessa.

Cominciamo qui dal dimostrare l'importante teorema:

Un'equazione $f(x) = 0$ è riducibile od irriducibile, secondo che il gruppo di GALOIS *è intransitivo ovvero transitivo.*

Supponiamo che il gruppo G di GALOIS sia intransitivo. Le n radici

$$x_1 x_2 \ldots x_n$$

di $f(x) = 0$ si scindono allora in sistemi di transitività, tali che le radici di ciascun sistema sono permutate transitivamente fra loro dalle sostituzioni di G (§. 9).

Siano

$$x_1 x_2 \ldots x_r \; (r < n)$$

le radici appartenenti ad un medesimo sistema; il fattore di $f(x)$

$$\varphi(x) = (x - x_1)(x - x_2) \ldots (x - x_r)$$

è razionalmente noto perchè le sostituzioni del gruppo di GALOIS, scambiando fra loro $x_1, x_2 \ldots x_r$, lasciano i suoi coefficienti numericamente invariati. Ne segue che la $f(x)$ è riducibile. Dunque, se $f(x) = 0$ è irriducibile, il gruppo di GALOIS deve essere transitivo.

Sarà evidentemente completata la dimostrazione del teorema se proviamo che, quando $f(x) = 0$ è riducibile, il gruppo G di GALOIS è necessariamente intransitivo.

Sia

$$\varphi(x) = (x - x_1)(x - x_2) \ldots (x - x_r)$$

un fattore di $f(x)$; qualunque valore α, appartenente al campo di razionalità, diamo alla x sarà $\varphi(\alpha)$ razionalmente noto e quindi dovendo $\varphi(\alpha) = (\alpha - x_1)(\alpha - x_2) \ldots (\alpha - x_r)$ rimanere numericamente invariata per qualunque sostituzione del gruppo di GALOIS, dovranno per tutte le sostituzioni di G scambiarsi $x_1, x_2, \ldots x_r$ fra loro, onde G è intransitivo.

§. 68. — Denotiamo con

$$f(x) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \ldots + c_{n-1} x + c_n = 0$$

l'equazione *generale* di grado n, dove dunque i coefficienti c restano in-

determinati. Quale sarà il gruppo di GALOIS della $f(x) = 0$ nel campo di razionalità $(c_1, c_2 \ldots c_n)$? È facile vedere che tale gruppo è il gruppo totale $G_{\pi(n)}$ sulle n radici. Ammesso infatti che ne fosse un sottogruppo

$$G_r = (s_1, s_2 \ldots s_r),$$

e indicando con

$$V_{s_1}, V_{s_2} \ldots V_{s_r}$$

le radici del primo fattore irriducibile della risolvente di GALOIS, una funzione simmetrica di queste, p. e.

$$F(x_1 x_2 \ldots x_n) = V_{s_1} + V_{s_2} + \ldots + V_{s_r},$$

che è funzione *non simmetrica* delle radici di $f(x) = 0$, sarebbe razionalmente esprimibile per $c_1 c_2 \ldots c_n$ ed eguale quindi ad una funzione *simmetrica* $\Phi(x_1 x_2 \ldots x_n)$ delle radici stesse. Una tale eguaglianza

$$F(x_1 x_2 \ldots x_n) = \Phi(x_1 x_2 \ldots x_n)$$

fra una funzione non simmetrica ed una simmetrica, restando indeterminate le c, quindi le x stesse è evidentemente assurda. Ma si può spingere molto più in là la ricerca e dimostrare che, persino nel campo assoluto di razionalità, si possono costruire infinite equazioni di un dato grado n qualunque, con coefficienti interi, il cui gruppo di GALOIS sia il gruppo totale [1].

Noi qui ci limiteremo a riportare la dimostrazione di WEBER [2]) pel caso in cui il grado n sia un numero primo. Costruiamo per ciò p. e. col processo del §. 60, un'equazione irriducibile

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$$

del dato grado primo n, i cui coefficienti siano numeri interi e supponiamo che il suo gruppo di GALOIS G, che è certamente transitivo per l'irriducibilità dell'equazione (§. 67), non coincida col gruppo totale.

Pel teorema alla fine del §. 13, il gruppo G di GALOIS non può contenere alcuna trasposizione. Se ora aggiungiamo al campo di razionalità $n-2$ delle radici di $f(x) = 0$, il gruppo si abbasserà (§. 66) al sottogruppo

---

[1]) V.i HILBERT. — *Journal von Crelle*, Bd. 110.

[2]) *Algebra*, Bd. I., pag. 605.

contenente quelle sostituzioni di G che non spostano queste $n-2$ radici, cioè si ridurrà all'identità; le altre due radici saranno quindi razionalmente esprimibili per quelle $n-2$, con coefficienti reali razionali. Ne segue che se un'equazione irriducibile di grado primo n, con coefficienti interi, ha un gruppo di Galois inferiore al gruppo totale ed ha $n-2$ radici reali, anche le altre due sono reali. Si ha dunque il teorema:

Un'equazione irriducibile di grado primo a coefficienti reali interi e con due sole radici immaginarie ha per gruppo di Galois *il gruppo totale.*

Così p. e. l'equazione di 5.° grado

$$f(x) = x^5 + p x^2 - p x - p = 0 ,$$

dove p è un numero primo qualunque, è irriducibile pel teorema al §. 60 ed ha una sola radice positiva, due negative [1]) e quindi due immaginarie, onde il suo gruppo di Galois è il gruppo totale.

È anche facile dimostrare l'esistenza di siffatte equazioni per un grado primo n qualunque. Si costruisca infatti un'equazione del grado primo dato n

$$f(x) = x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \ldots + \alpha_{n-1} x + \alpha_n = 0$$

con coefficienti reali che abbia $n-2$ radici reali e le altre due immaginarie, p. e.

$$(x-1)(x-2)\ldots(x-(n-2))(x^2+1) = 0 .$$

Aumentando i coefficienti α di quantità reali abbastanza piccole ε, variano, come si sa, di tanto poco quanto si vuole le radici e in particolare si può sempre fare in guisa che, mantenendo le ε in valore assoluto $< h$, essendo h una quantità abbastanza piccola, restino $n-2$ delle radici reali, le altre due immaginarie [2]). Ora possiamo prendere,

---

[1]) Ciò risulta subito dall'applicare la regola dei segni di Cartesio e dall'osservare che si ha

$$f(0) = -p < 0 , \quad f(-1) = p - 1 > 0 .$$

[2]) Suppongasi ad esempio che le $n-2$ radici reali di $f(x) = 0$ giacciano negli intervalli

$$(a_1 a_2) , \quad (a_2 a_3) \ldots (a_{n-2} a_{n-1})$$

di guisa che sia p. e.

$$f(a_1) < 0 , \quad f(a_2) > 0 , \quad f(a_3) < 0 \ldots f(a_{n-1}) > 0$$

in infiniti modi, i coefficienti interi

$$a_0 \quad a_1 \quad a_2 \ldots a_n$$

in guisa che $a_1, a_2 \ldots a_n$ siano divisibili per un numero primo p che non divida a_0 e sia a_n non divisibile per p^2 e in guisa inoltre che i rapporti

$$\frac{a_1}{a_0}, \frac{a_2}{a_4}, \ldots \frac{a_n}{a_0}$$

differiscano da

$$\alpha_1, \alpha_2 \ldots \alpha_n$$

rispettivamente meno di h. Allora l'equazione irriducibile

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

avrà due sole radici immaginarie.

§. 69. — Prendiamo una funzione razionale qualunque

$$y_1 = \psi(x_1, x_2 \ldots x_n)$$

delle radici della proposta. Quelle sostituzioni del gruppo G_r di GALOIS che lasciano y_1 *numericamente* invariata formano in G_r un sottogruppo (§. 66); sia

$$\Gamma_s = (\gamma_1, \gamma_2, \ldots \gamma_s)$$

questo sottogruppo che diremo il *sottogruppo numerico* della y_1. Essendo y_g il valore che assume y_1, effettuata entro y_1 sulle x la sostituzione g del gruppo di GALOIS, si vede che si avrà

$$y_g = y_{g'}$$

---

e sia H una quantità inferiore ai valori assoluti di $f(a_1), f(a_2) \ldots f(a_{n-1})$. Posto

$$\overline{f}(x) = x^n + (\alpha_1 + \varepsilon_1) x^{n-1} + (\alpha_2 + \varepsilon_2) x^{n-2} + \ldots + \alpha_n + \varepsilon_n ,$$

si prendano le ε tutte inferiori in valore assoluto a h, essendo h preso in guisa che sia

$$h \{ (a_i)^{n-1} + (a_i)^{n-2} + \ldots + (a_i) + 1 \} = h \frac{(a_i)^n - 1}{(a_i) - 1} < \mathrm{H} ;$$

avremo ancora

$$\overline{f}(a_1) < 0 \ , \ \overline{f}(a_2) > 0 \ , \ \overline{f}(a_3) < 0 \ldots$$

e la $\overline{f}(x) = 0$ avrà $n-2$ radici reali fra i medesimi limiti. Nè può la $\overline{f}(x) = 0$, se h è abbastanza piccolo, avere le altre due radici reali.

allora e allora soltanto quando si abbia

$$g' = \gamma_i g ,$$

cioè g' sia equivalente (a sinistra) a g, nel senso del §. 17, rispetto al sottogruppo Γ. E infatti alla identità

$$y_{g'} - y_g = 0 ,$$

applicando la sostituzione g^{-1} del gruppo di Galois, segue

$$y_{g' g^{-1}} = y_1 ,$$

indi $g' g^{-1} = \gamma_i$.

Ciò posto, ripartiamo le sostituzioni di G rispetto al sottogruppo Γ nel solito quadro

$$G = (\Gamma, \Gamma g_2 , \Gamma g_3 \ldots \Gamma g_q) ,$$

dove con q abbiamo denotato l'indice di Γ in G. I valori distinti che assume y_1 per le sostituzioni del gruppo di Galois sono dunque soltanto

$$(\alpha) \qquad y_1 , \; y_{g_2} , \; y_{g_3} \ldots y_{g_q} .$$

Se in questi q valori di y effettuiamo contemporaneamente una sostituzione g del gruppo di Galois essi diventano

$$y_g , \; y_{g_2 g} , \; y_{g_3 g} , \ldots y_{g_q g}$$

cioè si permutano fra loro precisamente secondo la corrispondente sostituzione del gruppo complementare (a destra)

$$H = \frac{G}{\Gamma} \quad (\text{V.}^{\text{i}} \S. 17).$$

Se costruiamo ora il polinomio razionale intero di grado q nella variabile y:

$$\varphi (y) = (y - y_1) \; (y - y_{g_2}) \; (y - y_{g_3}) \ldots (y - y_{g_q}) ,$$

i suoi coefficienti, come funzioni simmetriche dei q valori (α) che le sostituzioni di G permutano fra loro, sono funzioni razionali delle x numericamente invariabili per le sostituzioni del gruppo di Galois e quindi razionalmente note.

L'equazione

$$(7) \qquad \varphi \; (y) = 0 ,$$

che si può costruire razionalmeute ed ha per radici i q valori distinti (α) che assume la

$$y_1 = \psi(x_1\, x_2 \ldots x_n)$$

per le sostituzioni del gruppo di Galois, dicesi una *risolvente* della proposta. Se si aggiunge al campo di razionalità la prima radice y_1 della risolvente, il gruppo di Galois per la proposta scende da G a Γ (§. 66) e però qualunque altra funzione razionale z_1 delle radici della proposta, il cui sottogruppo numerico sia Γ stesso, sarà razionalmente nota. Ne risulta che se costruiamo due diverse risolventi della proposta con due funzioni razionali delle radici y_1, z_1 che abbiano il medesimo sottogruppo numerico, esse saranno trasformate di Tschirnhaus l'una dell'altra e, come nel caso particolare della risolvente di Galois (§. 63), saranno da noi riguardate come identiche.

Inversamente sia dato ad arbitrio un sottogruppo Γ del gruppo G di Galois; potremo sempre costruire una funzione razionale delle radici della proposta che abbia Γ per sottogruppo numerico. Pongasi infatti

$$\Gamma = (\gamma_1,\ \gamma_2 \ldots \gamma_s)$$

e indicando con V_g le radici del primo fattore irriducibile della risolvente di Galois si prenda

$$y_1 = (\rho - V_{\gamma_1})\,(\rho - V_{\gamma_2}) \ldots (\rho - V_{\gamma_s})\,,$$

ove ρ è un'indeterminata qualunque nel campo di razionalità. Per qualunque sostituzione γ di Γ la y_1 rimane invariata; per un'altra sostituzione g di G essa diventa

$$y_g = (\rho - V_{\gamma_1 g})\,(\rho - V_{\gamma_2 g}) \ldots (\rho - V_{\gamma_s g})\,.$$

Evitando particolari valori di ρ, potremo quindi sempre ottenere che il sottogruppo numerico di y_1 sia precisamente Γ.

Così: *Ad ogni sottogruppo* Γ *del gruppo di* Galois *corrisponde una classe di risolventi della proposta costruite con funzioni razionali delle radici della primitiva a sottogruppo numerico* Γ, *che sono trasformate di* Tschirnhaus *l'una dell'altra.*

Si osservi poi che, essendo Γ il sottogruppo numerico di y_1, il sottogruppo numerico di y_g, essendo g una qualunque sostituzione di G,

sarà precisamente il gruppo trasformato $\Gamma' = g^{-1}\,\Gamma\,g$. E infatti da

$$y_{g\,g'} = y_g$$

segue

$$y_1 = y_{g\,g'\,g^{-1}}\,,$$

indi

$$g\,g'\,g^{-1} = \gamma_i\,, \quad g' = g^{-1}\,\gamma_i\,g\,.$$

I sottogruppi numerici delle varie radici della risolvente sono quindi affini fra loro nel gruppo. Viceversa a due sottogruppi affini di G corrispónde la medesima risolvente.

§. 70. — È importante risolvere la questione: *Quale è il gruppo di* Galois *per la risolvente* (7) $\varphi(y) = 0$?

Si è già visto che le sostituzioni del gruppo di Galois inducono sulle radici (α) della risolvente

$$y_1\; y_{g_2} \ldots y_{g_q}$$

precisamente le sostituzioni del gruppo complementare $H = \frac{G}{\Gamma}$ ed ora dimostriamo facilmente il teorema:

La risolvente $\varphi(y) = 0$, *costruita con una funzione razionale* y_1 *delle radici della proposta a sottogruppo numerico* Γ, *ha precisamente per gruppo di* Galois *il gruppo complementare* $H = \frac{G}{\Gamma}$ *del gruppo* G *della proposta rispetto al sottogruppo numerico* Γ.

E infatti una funzione razionale

$$U\,(y_1, y_{g_2} \ldots y_{g_q})$$

delle radici della risolvente, è altresì una funzione razionale delle radici della proposta

$$U\,(y_1, y_{g_2}, \ldots y_{g_q}) = F\,(x_1, x_2 \ldots x_n)$$

e in questa relazione è lecito eseguire qualunque sostituzione g del gruppo di Galois. Ora una g, eseguita sulla x, induce sulle y la corrispondente sostituzione h di H. Quindi, se U è razionalmente nota, essa rimane numericamente invariata per tutte le h e viceversa, se U rimane numericamente invariata per tutte le h, essa è razionalmente nota. Dunque H è precisamente il gruppo di Galois della risolvente (§. 65).

Evidentemente H è sempre transitivo e per ciò: *le risolventi* $\varphi(y) = 0$, *costruite nel modo del §. 69, sono sempre irriducibili.*

Supponiamo ora di avere completamente risoluta la risolvente $\varphi(y) = 0$, cioè di conoscere *tutte* le sue radici. Quale vantaggio avremo ottenuto per la risoluzione della proposta? Il suo gruppo G di Galois si troverà abbassato (§. 66) a quel sottogruppo Σ che lascia singolarmente invariato il valor numerico di ciascuna radice della risolvente, cioè a quelle sostituzioni di G che corrispondono all'identità in H, ovvero alle sostituzioni comuni a Γ e a tutti i sottogruppi affini in G (§. 17). In ogni caso Σ è invariante in G, talchè, quando G è un gruppo semplice, Σ è l'identità. Allora colla risoluzione della risolvente $\varphi(y) = 0$ è anche risoluta la proposta; ma si noti che in tal caso i gruppi G, H della proposta e della risolvente sono oloedricamente isomorfi.

§. 71. — Abbiamo esaminato (§. 67) quali proprietà della equazione corrispondono alla transitività o intransitività del gruppo di Galois. Esaminiamo ora quali sono le proprietà di un'equazione a gruppo imprimitivo. Se le n radici di $f(x) = 0$ si ripartiscono in r sistemi di imprimitività, contenenti ciascuno s radici, talchè $n = rs$, distinguiamo per comodità le radici con un doppio indice di cui il primo si riferisce al sistema d'imprimitività, il secondo al posto che vi occupa la radice. Così distribuiamo le n radici nel quadro

$$\left\| \begin{matrix} x_{11} & x_{12} & \cdots & x_{1s} \\ x_{21} & x_{22} & \cdots & x_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ x_{r1} & x_{r2} & \cdots & x_{rs} \end{matrix} \right\| ,$$

le cui orizzontali rappresentano i sistemi d'imprimitività. Prendiamo ora una funzione razionale simmetrica delle radici della prima orizzontale p. e.

$$y_1 = (\rho - x_{11})(\rho - x_{12}) \ldots (\rho - x_{1s}) ,$$

essendo ρ una costante arbitrariamente scelta nel campo di razionalità. I valori numericamente distinti che y_1 assumerà saranno al più gli r valori

$$y_i = (\rho - x_{i1})(\rho - x_{i2}) \ldots (\rho - x_{i3})$$
$$(i = 1, 2, \ldots r)$$

e noi supporremo appunto ρ scelta in guisa che questi r valori siano distinti ciò che è sempre possibile, evitando al solito un numero finito di valori per ρ. Costruiamo ora la risolvente

$$\varphi(y) = (y - y_1)(y - y_2) \ldots (y - y_r) = 0,$$

il cui gruppo sarà (§. 70) il gruppo H indotto da G sui sistemi di imprimitività. Se aggiungiamo al campo di razionalità la radice y_1 della $\varphi(y) = 0$, il gruppo G della proposta si abbassa a quel sottogruppo che lascia fermo il primo sistema d'imprimitività e però il fattore

$$(x - x_{11})(x - x_{12}) \ldots (x - x_{1s})$$

ne viene separato razionalmente; si ha cioè

$$(x - x_{11})(x - x_{12}) \ldots (x - x_{1s}) = x^s + \alpha_1(y_1) x^{s-1} + \alpha_2(y_1) x^{s-2} + \ldots + \alpha_s(y_1),$$

dove le α sono razionali intere in y_1 con coefficienti appartenenti al campo primitivo di razionalità. Eseguendo sull'identità precedente una sostituzione dell'antico gruppo G di Galois, che porti il 1.° sistema di imprimitività nell'i^{mo}, avremo:

$$(x - x_{i1})(x - x_{i2}) \ldots (x - x_{is}) = x^s + \alpha_1(y_i) x^{s-1} + \alpha_2(y_i) x^{s-2} + \ldots + \alpha_s(y_i)$$
$$i = 1, 2, 3 \ldots r.$$

Abbiamo quindi

$$f(x) = \prod_{i=1}^{i=r} \left\{ x^s + \alpha_1(y_i) x^{s-1} + \alpha_2(y_i) x^{s-2} + \ldots + \alpha_s(y_i) \right\}$$

e possiamo enunciare il resultato:

L'equazione $f(x) = 0$, a gruppo imprimitivo, si ottiene eliminando y fra le due equazioni

$$\begin{cases} \varphi(y) = y^r + c_1 y^{r-1} + c_2 y^{r-2} + \ldots + c_{r-1} y + c_r = 0 \\ x^s + \alpha_1(y) x^{s-1} + \alpha_2(y) x^{s-2} + \ldots + \alpha_s(y) = 0 . \end{cases}$$

Viceversa è facile vedere che ogni equazione ottenuta in questo modo ha un gruppo imprimitivo.

Osserviamo infine che, risoluta la risolvente $\varphi(y) = 0$ che scinde i sistemi d'imprimitività, i singoli fattori irriducibili

$$(x - x_{i1})(x - x_{i2}) \ldots (x - x_{is}) = 0$$

di $f(x) = 0$ hanno gruppi di Galois simili fra loro. E infatti se Γ è il

sottogruppo di G che lascia fermo il 1.° sistema, g una sostituzione di G che porta questo sistema nell'i^{mo}, sarà $g^{-1}\Gamma g$ il sottogruppo che lascia fermo questo i^{mo} sistema, ossia sarà $g^{-1}\Gamma g$ il gruppo di GALOIS per l'equazione

$$(x - x_{i_1})(x - x_{i_2})\ldots(x - x_{i_s}) = 0\,.$$

§. 72. — Arriviamo ora alla parte più importante delle teorie di GALOIS, a ricercare cioè come la *composizione* del gruppo di GALOIS si rifletta in corrispondenti proprietà della equazione. Per esprimerci con maggior brevità diremo *semplice* o *composta* un'equazione (in un dato campo di razionalità) secondo che il suo gruppo di GALOIS è semplice o composto. Dimostriamo l'importante teorema:

Alla risoluzione di un'equazione composta $f(x) = 0$ può sostituirsi la successiva risoluzione di equazioni ausiliarie semplici.

Sia G il gruppo di GALOIS della proposta e, supponendolo composto, indichiamo con G_1 un suo sottogruppo invariante massimo. Prendiamo, secondo il §. 69, una funzione razionale

$$y_1 = \psi(x_1 x_2 \ldots x_n)$$

delle radici della proposta il cui sottogruppo numerico sia precisamente G_1 e con essa costruiamo la corrispondente risolvente

$$\varphi_{e_1}(y) = 0\,,$$

il cui grado e_1 eguaglierà l'indice di G_1 in G. Il gruppo di questa risolvente sarà (§. 70) il gruppo *fattoriale*

$$H_1 = \frac{G}{G_1}\,,$$

che è un gruppo semplice (§. 21). Il gruppo H_1 transitivo sulle e_1 radici

$$y_1\, y_2 \ldots y_{e_1}$$

della risolvente ha un ordine precisamente eguale ad e_1; esso è quindi semplicemente transitivo e nessuna sua sostituzione, tranne l'identità, lascia ferma una radice. Ne segue che qualunque radice di $\varphi_{e_1}(y) = 0$ è razionalmente esprimibile per una radice fissa arbitraria, cioè: *la risolvente $\varphi_{e_1}(y) = 0$ è un'equazione normale.*

Se supponiamo risoluta la risolvente

$$\varphi_{e_1}(y) = 0,$$

per il che basterà conoscere ed aggiungere al campo di razionalità una sua radice, il gruppo della proposta scende da G al sottogruppo invariante massimo G_1.

Partendo ora dal nuovo campo di razionalità in cui il gruppo di $f(x) = 0$ è G_1, prendiamo un sottogruppo invariante massimo G_2 in G_1, e sia e_2 il corrispondente fattore di composizione; costruiremo nel medesimo modo una nuova risolvente

$$\varphi_{e_2}(z) = 0,$$

che sarà un'equazione normale semplice, il cui gruppo coinciderà col gruppo fattoriale $\frac{G_1}{G_2}$. La risoluzione di $\varphi_{e_2}(z) = 0$, cioè la conoscenza di una sua radice, abbassa il gruppo della proposta da G_1 a G_2. Così continuando, arriviamo all'importante risultato:

Se l'equazione proposta $f(x) = 0$ *ha per gruppo di* Galois *un gruppo composto* G, *di cui sia*

$$G, G_1, G_2 \ldots G_\nu, 1$$

una serie di composizione, coi fattori di composizione

$$e_1, e_2, \ldots e_\nu,$$

la sua risoluzione si riduce a quella di successive risolventi normali semplici

$$\varphi_{e_1}(y) = 0, \varphi_{e_2}(z) = 0 \ldots \varphi_{e_\nu}(t) = 0,$$

i cui gradi coincidono coi rispettivi fattori di composizione e i corrispondenti gruppi sono i gruppi fattoriali di G.

In qualunque modo si riduca così la risoluzione di un'equazione composta a quelle di successive risolventi semplici, i teoremi di Jordan e di Hölder sull'invariabilità dei fattori di composizione e dei gruppi fattoriali (§§. 19, 21) ci dimostrano che gli ordini di queste equazioni ausiliarie e i loro gruppi di Galois rimangono sempre gli stessi.

CAPITOLO VI.

Equazioni Abeliane. — Condizioni di risolubilità di un'equazione per radicali. — Risolventi di grado $\leq n$ dell'equazione generale di grado n. — Equazioni di grado primo risolubili. — Risolvente di LAGRANGE.

§. 73. — Andiamo ora ad applicare le teorie generali fin qui esposte ad un'importante classe di equazioni che per primo ABEL considerò e che portano per ciò il nome di *equazioni Abeliane*. Chiamiamo Abeliana ogni equazione il cui gruppo di GALOIS sia un gruppo Abeliano (§. 30), cioè un gruppo le cui sostituzioni siano due a due permutabili.

Se l'equazione Abeliana

$$f(x) = 0$$

è riducibile, essa si scinde nel prodotto di più equazioni Abeliane irriducibili.

E infatti se le n radici si dividono in più sistemi di transitività

$$[x_1 x_2 \ldots x_i]$$
$$[x_{i+1} \ldots x_k]$$
$$\ldots\ldots$$

ciascuna sostituzione del gruppo Abeliano G sarà il prodotto di altrettante sostituzioni prese da gruppi Abeliani transitivi

$$\Gamma, \Gamma', \Gamma'' \ldots$$

sulle radici di ciascun sistema e i corrispondenti fattori irriducibili di $f(x)$:

$$f_1(x) = (x - x_1) \quad (x - x_2) \quad \ldots (x - x_i)$$
$$f_2(x) = (x - x_{i+1}) \; (x - x_{i+2}) \ldots (x - x_k)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

eguagliati a zero daranno altrettante equazioni Abeliane coi gruppi parziali

$$\Gamma, \Gamma', \Gamma'' \ldots$$

Ora, supposta l'equazione Abeliana di grado n

$$f(x) = 0$$

irriducibile, facilmente vediamo che il suo gruppo transitivo G è pre-

cisamente d'ordine n. E infatti se una sostituzione g di G lascia ferma una radice p. e. x_1, vi sarà in G una sostituzione γ che trasporta x_1 nella radice arbitraria x_i e la $\gamma^{-1} g \gamma = g$ lascierà ferma x_i; ne segue che g è l'identità. L'ordine di G è dunque uguale a n (§. 10) e noi indicheremo con g_i quella sua sostituzione, perfettamente determinata, che porta x_1 in x_i. Se ora aggiungiamo al campo di razionalità una radice, p. e. x_1, il gruppo di Galois si abbasserà all'identità (§. 66) e tutte le altre radici saranno razionalmente note. Avremo quindi in particolare

$$x_i = \theta_i(x_1) \ , \ x_k = \theta_k(x_1) \ ,$$

dove θ_i, θ_k sono funzioni razionali, che possono supporsi intere e di grado $n-1$ al più. Sia x_l la radice in cui il prodotto

$$g_i g_k = g_k g_i$$

porta la x_1. Applicando alle relazioni

$$x_i - \theta_i(x_1) = 0 \ , \ x_k - \theta_k(x_1) = 0$$

rispettivamente le sostituzioni g_k, g_i del gruppo di Galois, ne deduciamo

$$x_l - \theta_i(\theta_k(x_1)) = 0 \ , \ x_l - \theta_k(\theta_i(x_1)) = 0 \ ,$$

cioè

$$\theta_i(\theta_k(x_1)) = \theta_k(\theta_i(x_1)) \ .$$

Abbiamo dunque il teorema:

Ogni equazione Abeliana irriducibile è un'equazione normale, cioè per una sua radice qualunque, p. e. x_1, *tutte le altre sono razionalmente esprimibili; inoltre se* $\theta_i(x_1)$, $\theta_k(x_1)$ *sono due radici qualunque, si ha*

$$\theta_i(\theta_k(x_1)) = \theta_k(\theta_i(x_1)) \ ,$$

ossia le operazioni θ, *eseguite sulle radici, sono due a due invertibili.*

Inversamente è facile dimostrare che, se per un'equazione normale irriducibile le operazioni razionali θ, che applicate ad una radice danno le altre, sono due a due invertibili, l'equazione sarà Abeliana. Anzi basterà supporre che per una radice fissa x_1 dell'equazione irriducibile siano esprimibili razionalmente tutte le altre, mediante operazioni θ due a due permutabili, perchè ne segua che l'equazione è Abeliana e la proprietà supposta per la radice x_1 ha quindi luogo per ogni altra radice. E infatti poichè, aggiunta x_1 al campo di razionalità, l'equazione è risoluta

il gruppo transitivo G sarà d'ordine n e potremo, come sopra, indicare con g_i la sostituzione che porta x_1 in x_i. Si abbia ora

$$(1) \qquad x_i - \theta_i(x_1) = 0 \,.\, x_k - \theta_k(x_1) = 0\,;$$

indicando con x_r la radice in cui x_1 è portata da $g_i g_k$, con x_s quella in cui è portata da $g_k g_i$ ed operando sulle due relazioni (1) rispettivamente con g_k, g_i ne dedurremo

$$x_r = \theta_i(\theta_k(x_1)) \,.\, x_s = \theta_k(\theta_i(x_1))\,,$$

quindi, per la permutabilità supposta delle operazioni θ

$$x_r = x_s\,, \quad r = s\,.$$

Dunque $g_i g_k$, $g_k g_i$ portando x_1 nella medesima radice x_r sono identiche:

$$g_i g_k = g_k g_i$$

ed il gruppo è in conseguenza Abeliano, c. d. d.

§. 74. — Se applichiamo il risultato finale del §. 72 ad un'equazione Abeliana composta, vediamo subito che le successive equazioni ausiliarie semplici (risolventi) saranno anch'esse Abeliane ed inoltre i loro gradi, eguagliando i fattori di composizione del gruppo, saranno altrettanti numeri primi (§. 30). Alla risoluzione di un'equazione Abeliana di grado composto $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ si può quindi sostituire quella di altrettante equazioni Abeliane di grado primo e precisamente di α_1 equazioni di grado p_1, α_2 di grado p_2 ecc.

Basterà dunque occuparsi della risoluzione di un'equazione Abeliana irriducibile di grado primo Il gruppo di una tale equazione consta evidentemente delle p potenze di una sostituzione ciclica sulle p radici; ma noi generalizziamo la ricerca considerando la risoluzione di un'equazione Abeliana di grado qualsiasi n ma il cui gruppo consti delle n potenze di una sostituzione ciclica sulle n radici

$$S = (x_0 x_1 x_2 \ldots x_{n-1})\,,$$

che qui prendiamo per comodità cogli indici

$$0, 1, 2, \ldots n-1$$

presi (mod n), e riguardiamo quindi $x_r = x_s$ quando $r \equiv s$ (mod n). In

altre parole noi ci occupiamo qui della risoluzione di un'equazione Abeliana irriducibile il cui gruppo abbia una base di un solo termine. È chiaro che, rappresentando il gruppo Abeliano di un'equazione Abeliana qualunque per mezzo di una base

$$[g_1 g_2 \ldots g_r]$$

al modo del §. 33, ed applicando il processo del §. 72 ai gruppi

$$G = [g_1 g_2 \ldots g_r], \quad G_1 = [g_2 g_3 \ldots g_r], \quad G_2 = [g_3 \ldots g_r] \ldots$$

ridurremo appunto la risoluzione dall'equazione Abeliana a quella di successive equazioni Abeliane a gruppo ciclico, di gradi n_1, n_2, $n_3 \ldots$

Consideriamo dunque la nostra equazione Abeliana

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n = 0,$$

il cui gruppo è

$$G = (1, S, S^2 \ldots S^{n-1})$$

con

$$S = (x_0 x_1 x_2 \ldots x_{n-1}).$$

Sia

$$x_1 = \theta(x_0),$$

essendo θ una funzione razionale intera di grado $< n$. Applicando alla relazione precedente la S e le sue potenze e ponendo per brevità

$$\theta(\theta(x_0)) = \theta^2(x_0), \quad \theta(\theta^2(x_0)) = \theta^3(x_0) \ldots,$$

troviamo

$$x_1 = \theta(x_0), \quad x_2 = \theta^2(x_0), \ldots x_{n-1} = \theta^{n-1}(x_0), \quad x_0 = \theta^n(x_0).$$

Le radici della equazione Abeliana formano in tal caso, come si dice, un unico periodo. Viceversa si vede subito che se le radici di un'equazione Abeliana irriducibile formano, convenientemente ordinate, un unico periodo

$$x_0, \quad \theta(x_0), \quad \theta^2(x_0) \ldots \theta^{n-1}(x_0),$$

il gruppo dell'equazione sarà il gruppo ciclico generato dalla sostituzione

$$S = (x_0, \theta(x_0), \theta^2(x_0) \ldots \theta^{n-1}(x_0)).$$

Indicando con ε una radice n^{ma} qualsiasi dell'unità, che aggiungiamo al campo di razionalità ove già non vi figuri, consideriamo la funzione

razionale delle radici della proposta

$$y_1 = x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \ldots + \varepsilon^{n-1} x_{n-1},$$

per la quale adottiamo la notazione

$$(\varepsilon_1 x_0) = x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \ldots + \varepsilon^{n-1} x_{n-1}.$$

Se a questa funzione y_1 razionale nelle radici della proposta applichiamo la sostituzione fondamentale S del gruppo di Galois, otteniamo

$$y_s = x_1 + \varepsilon x_2 + \varepsilon^2 x_3 + \ldots + \varepsilon^{n-1} x_0 = \varepsilon^{-1} y_1,$$

onde segue che la sua n^{ma} potenza

$$y_1{}^n = (\varepsilon, x_0)^n$$

rimane numericamente invariata applicandovi la S e le sue potenze e però essa è razionalmente esprimibile per le quantità primitive del campo di razionalità e per ε.

Ora diamo ad ε il significato di una radice *primitiva* n^{ma} dell'unità e poniamo

$$(\varepsilon^r, x_0)^n = B_r; \tag{2}$$

queste quantità B_r saranno tutte razionalmente note e però le (ε^r, x_0) si otterranno estraendo una radice n^{ma}. Dalle n equazioni lineari

$$(3)\quad \begin{cases} (1, x_0) = x_0 + x_1 + x_2 + \ldots + x_{n-1} = -a_1 \\ (\varepsilon, x_0) = x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \ldots + \varepsilon^{n-1} = \sqrt[n]{B_1} \\ (\varepsilon^2, x_0) = x_0 + \varepsilon^2 x_2 + \varepsilon^4 x_2 + \ldots + \varepsilon^{2(n-1)} x_{n-1} = \sqrt[n]{B_2} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (\varepsilon^{n-1}, x_0) = x_0 + \varepsilon^{n-1} x_1 + \varepsilon^{2(n-1)} x_2 + \ldots + \varepsilon^{(n-1)2} x_{n-1} = \sqrt[n]{B_{n-1}} \end{cases}$$

sommando, coll'osservare che per $r \not\equiv 0 \pmod{n}$ si ha

$$1 + \varepsilon^r + \varepsilon^{2r} + \ldots + \varepsilon^{(n-1)r} = \frac{\varepsilon^{nr} - 1}{\varepsilon^r - 1} = 0, \tag{4}$$

risulta

$$x_0 = \frac{-a_1 + \sqrt[n]{B_1} + \sqrt[n]{B_2} + \ldots + \sqrt[n]{B_{n-1}}}{n}, \tag{A}$$

la quale formola ci fa conoscere con estrazione di radicali la prima ra-

dice x_0. Le altre possono dedursi razionalmente da x_0, ma si calcolano anche dalle equazioni lineari stesse (3). Moltiplicandole ordinatamente per $1, \varepsilon^{-r}, \varepsilon^{-2r}, \ldots \varepsilon^{-(n-1)r}$, coll'osservare la (4), si ha

$$(A^*) \qquad x_r = \frac{-a_1 + \varepsilon^{-r}\sqrt[n]{B_1} + \varepsilon^{-2r}\sqrt[n]{B_r} + \ldots + \varepsilon^{-(n-1)r}\sqrt[n]{B_{n-1}}}{n}$$

$$r = 0,\ 1,\ 2 \ldots n-1 .$$

Ciascuno degli $n-1$ radicali che figurano in questa formola di risoluzione è suscettibile di n diverse determinazioni; ma, come ora dimostreremo, basterà dare al primo radicale i suoi n valori, i rimanenti radicali potendosi esprimere razionalmente pel primo.

§. 75. — Per compiere la richiesta modificazione della formola (A), basta risalire al significato che, secondo la formola (2), ha per noi

$$\sqrt[n]{B_r} = (\varepsilon^r, x_0) .$$

Applicando la sostituzione fondamentale S la funzione (ε, x_0) si moltiplica, come abbiamo visto, per ε^{-1} e similmente la (ε^r, x_0) per ε^r, onde il prodotto

$$(\varepsilon^r, x_0)\,(\varepsilon, x_0)^{n-r} = \sqrt[n]{B_r}\,(\sqrt[n]{B_1})^{n-r}$$

è razionalmente noto. Poniamo dunque

$$\sqrt[n]{B_r}\,(\sqrt[n]{B_1})^{n-r} = c_r ,$$

essendo c_r una quantità razionalmente nota (nel campo ampliato con ε). Supponendo dunque che sia

$$\sqrt[n]{B_1} = (\varepsilon, x_0) \neq 0 ,$$

avremo

$$\sqrt[n]{B_r} = \frac{c_r}{B_1}(\sqrt[n]{B_1})^r$$

e la formola (A) di risoluzione prenderà la nuova forma

$$(B) \qquad x_0 = \frac{1}{n}\left\{-a_1 + \sqrt[n]{B_1} + \frac{c_2}{B_1}(\sqrt[n]{B_1})^r + \frac{c_3}{B_1}(\sqrt[n]{B_1})^3 + \ldots + \frac{c_{n-1}}{B_1}(\sqrt[n]{B_1})^{n-1}\right\},$$

nella quale dando a $\sqrt[n]{B_1}$ i suoi n valori si otterranno, come subito si vede, tutte le n radici.

La trasformazione della formola (A) nella (B) suppone, come sopra si è avvertito, che non sia

$$(\varepsilon, x_0) = 0 .$$

Quando questo caso eccezionale si presenti si potrebbe ricorrere alla riduzione della equazione Abeliana a successive equazioni di grado primo, ove il caso eccezionale non può presentarsi [1]). In modo migliore si elimina la difficoltà col procedimento seguente dovuto a Weber [2]). Essendo ε una radice primitiva n^{ma} dell'unità e p un fattore primo di n, è facile vedere che può sempre scegliersi un conveniente esponente $\lambda \not\equiv 0 \pmod{p}$ tale che sia

$$(\varepsilon^\lambda , x_0) \neq 0 .$$

Si ha infatti

$$n\, x_0 = \sum_{\lambda=0}^{\lambda=n-1} (\varepsilon^\lambda , x_0)$$

$$n\, x_r = \sum_{\lambda=0}^{\lambda=n-1} \varepsilon^{-\lambda r} (\varepsilon^\lambda , x_0) ,$$

da cui

$$n\,(x_r - x_0) = \sum_{\lambda=0}^{\lambda=n-1} (\varepsilon^{-\lambda r} - 1)\, (\varepsilon^\lambda , x_0) .$$

Ponendo $n = pq$ si avrà in particolare

$$n\,(x_q - x_0) = \sum_{\lambda=0}^{\lambda=n-1} (\varepsilon^{-\lambda q} - 1)\, (\varepsilon^\lambda , x_0);$$

il primo fattore, sotto il segno Σ, $\varepsilon^{-\lambda q} - 1$ si annulla tutte le volte che $\lambda \equiv 0 \pmod{p}$ e se il secondo si annullasse sempre quando $\lambda \not\equiv 0$

---

[1]) Per n primo le potenze ε^r di ε con $r \not\equiv 0 \pmod{n}$ sono tutte primitive e se fosse sempre

$$(\varepsilon^r , x_0) = 0 \quad r = 1, 2, \ldots n-1$$

la (A*) darebbe per ogni radice il valore razionale $\frac{a_1}{n}$.

[2]) *Algebra.* — Bd. I, pag. 547.

(mod p) ne seguirebbe $x_q = x_0$ e la proposta irriducibile avrebbe radici eguali ciò che è assurdo [1]).

Ciò premesso, decompongasi n nei suoi fattori primi e sia

$$n = p_1^{\alpha_1} \; p_2^{\alpha_2} \ldots p_r^{\alpha_r} \; ;$$

poniamo inoltre per brevità

$$n_1 = \frac{n}{p_1^{\alpha_1}} \, , \; n_2 = \frac{n}{p_2^{\alpha_2}} \, , \ldots n_r = \frac{n}{p_r^{\alpha_r}}$$

e scegliamo, secondo le osservazioni superiori, gli esponenti

$$\lambda_1 \not\equiv 0 \pmod{p_1} \, , \; \lambda_2 \not\equiv 0 \pmod{p_2} \ldots \lambda_r \not\equiv 0 \pmod{p_r}$$

in guisa che sia

$$(\varepsilon^{\lambda_1}, x_0) \neq 0 \, , \; (\varepsilon^{\lambda_2}, x_0) \neq 0 \ldots (\varepsilon^{\lambda_r}, x_0) \neq 0 \, .$$

Le quantità $(\varepsilon^{\lambda_1}, x_0)^{n_1 p_1^{\alpha_1}}$, $(\varepsilon^{\lambda_2}, x_0)^{n_2 p_2^{\alpha_2}} \ldots$ sono razionalmente note; indicandone i valori con $\gamma_1, \gamma_2, \ldots \gamma_r$ avremo

$$(\varepsilon^{\lambda_1} \, , \; x_0)^{n_1} = \sqrt[p_1^{\alpha_1}]{\gamma_1} \; , \; (\varepsilon^{\lambda_2} \, , \; x_0)^{n_2} = \sqrt[p_2^{\alpha_2}]{\gamma_2} \ldots (\varepsilon^{\lambda_r}, x_0) = \sqrt[p_r^{\alpha_r}]{\gamma_r} \; .$$

È facile ora esprimere razionalmente una qualunque quantità

$$(\varepsilon^s \, , \; x_0) = \sqrt[n]{B_s}$$

razionalmente per i precedenti radicali. Si osservi per ciò che la funzione razionale delle radici

$$z_s = (\varepsilon^s, \, x_0) \, (\varepsilon^{\lambda_1}, \; x_0)^{n_1 \nu} \, (\varepsilon^{\lambda_2}, \, x_0)^{n_2 \nu} \ldots (\varepsilon^{\lambda_r}, \, x_0)^{n_r \nu}$$

acquista per la sostituzione S il fattore

$$\varepsilon^{-(\lambda_1 n_1 + \lambda_2 n_2 + \ldots + \lambda_r n_r)\nu - s}$$

onde, se determiniamo ν in guisa che sia

$$(\lambda_1 n_1 + \lambda_2 n_2 + \ldots + \lambda_r n_r) \, \nu \equiv - s \pmod{n} \, ,$$

---

[1]) Questa considerazione di WEBER dimostra che il caso eccezionale non può mai presentarsi quando n è la potenza di un numero primo.

la z_s sarà razionalmente nota. La congruenza superiore è sempre risolvibile perchè

$$\lambda_1 n_1 + \lambda_2 n_2 + \ldots + \lambda_r n_r$$

è primo con n. Avremo dunque:

$$\sqrt[n]{B_s} = (\varepsilon^s, x_0) = \frac{z_s}{\left(\sqrt[p_1^{\alpha_1}]{\gamma_1}\ \sqrt[p_2^{\alpha_2}]{\gamma_2} \ldots \sqrt[p_r^{\alpha_r}]{\gamma_r}\right)^{\nu}}.$$

Sostituendo questi valori di $\sqrt[n]{B_s}$ $(s = 1, 2 \ldots n-1)$ nella formola (A) di risoluzione e dando ai radicali

$$\sqrt[p_1^{\alpha_1}]{\gamma_1},\ \sqrt[p_2^{\alpha_2}]{\gamma_2} \ldots \sqrt[p_r^{\alpha_r}]{\gamma_r}$$

i loro valori diversi, si avranno nuovamente tutte le radici. Possiamo quindi enunciare il risultato finale col teorema:

Un'equazione Abeliana a gruppo ciclico sulle n radici si risolve aggiungendo al campo di razionalità una radice primitiva n^{ma} dell'unità ed estraendo un radicale d'indice n.

§. 76. — Siccome la risoluzione di un'equazione Abeliana qualsiasi si può ridurre a quella di successive equazioni Abeliane a gruppo ciclico abbiamo poi il teorema generale:

Ogni equazione Abeliana è risolubile per radicali.

Ma possiamo precisare di più quali radicali saranno da estrarsi per la risoluzione e dimostrare che, *ordinando convenientemente la formola di risoluzione, i radicali saranno separati cioè non porteranno l'uno sull'altro.* Determiniamo per ciò, secondo il §. 33, una base

$$[g_1 g_2 g_3 \ldots g_r]$$

del gruppo G di Galois e siano

$$n_1, n_2, n_3 \ldots n_r$$

i periodi rispettivi delle sostituzioni generatrici, cioè gli *invarianti* del gruppo Abeliano che diremo anche *gli invarianti dell'equazione Abeliana.* Consideriamo i sottogruppi di G

$$G_1 = [g_2 g_3 \ldots g_r],\ G_2 = [g_1 g_3 \ldots g_r] \ldots G_r = [g_1 g_2 \ldots g_{r-1}]$$

e per ciascuno di essi prendiamo una funzione razionale delle radici della proposta che resti numericamente invariata per le sole sostituzioni del rispettivo sottogruppo. Costruiremo così altrettante risolventi Abeliane della proposta dei rispettivi gradi

$$n_1, n_2, n_3 \ldots n_r;$$

ciascuna di esse, pei risultati generali dei §§. 69, 70, sarà a gruppo ciclico. Risolveremo quindi, pel §. precedente, queste successive ausiliarie ampliando il campo di razionalità coll'aggiunta di una radice primitiva ε dell'unità d'ordine n_1, dopo di che saranno note anche tutte le radici dell'unità di ordini $n_2, n_3, \ldots n_r$ che sono divisori di n_1 ed estraendo quindi r radicali separati

$$\sqrt[n_1]{A_1}, \sqrt[n_2]{A_2}, \ldots \sqrt[n_r]{A_r},$$

le quantità sotto il segno essendo note nel campo di razionalità ampliato coll'aggiunta di ε. Ma coll'estrazione di questi r radicali *separati* anche la proposta è risoluta. Infatti il suo gruppo si riduce (§. 66) al sottogruppo comune di G_1, $G_2 \ldots G_r$ che è l'identità.

Abbiamo dunque il teorema finale:

Per risolvere in un campo di razionalità (R, R′, R″ . . .) *un'equazione Abeliana di invarianti*

$$n_1, n_2, \ldots n_r$$

si aggiungerà al campo di razionalità una radice primitiva ε *dell'unità d'ordine eguale al primo invariante, e si estrarranno* r *radicali separati*

$$\sqrt[n_1]{A_1}, \sqrt[n_2]{A_2} \ldots \sqrt[n_r]{A_r}$$

di indici eguali ai rispettivi invarianti del gruppo, le quantità sotto il segno essendo razionali nel campo ampliato (R, R′, R″ . . . ε).

§. 77. — Supponiamo ora che un'equazione Abeliana a gruppo ciclico abbia i coefficienti reali e il campo di razionalità stesso sia pure *reale*, nel qual caso la funzione $\theta(x_0)$ sarà pure a coefficienti reali. Allora si può dare, secondo Abel, alla formola (B) di risoluzione, una forma particolare molto notevole. Noi supporremo qui senz'altro che il caso ec-

cezionale (§. 75) non si presenti; in tal caso si giungerebbe al medesimo risultato mediante considerazioni analoghe a quelle del §. citato [1]).

Osserviamo per ciò che se l'equazione Abeliana ha una radice reale (come accade certamente se il grado n dell'equazione è dispari) tutte le altre radici, come funzioni reali a coefficienti reali di questa, saranno pure reali. Allora le due quantità

$$\sqrt[n]{B_1} = (\varepsilon, x_0) = x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \ldots + \varepsilon^{n-1} x_{n-1}$$

$$\sqrt[n]{B_{n-1}} = (\varepsilon^{-1}, x_0) = x_0 + \varepsilon^{-1} x_1 + \varepsilon^{-2} x_2 + \ldots + \varepsilon^{-(n-1)} x_{n-1}$$

saranno coniugate. Ma se una delle radici della equazione è immaginaria, quindi tutte le altre, allora dimostriamo che l'una di queste quantità è eguale alla coniugata dell'altra cangiata di segno. E invero se supponiamo che la coniugata di x_0 sia x_k, da

$$x_\nu = \theta^\nu (x_0)$$

segue

$$x_{\nu+k} = \theta^\nu (x_k)$$

e però x_ν ha per coniugata $x_{\nu+k}$. Facendo $\nu = k$, sarà x_{2k} coniugata di x_k indi

$$x_{2k} = x_0$$

onde

$$k = \frac{n}{2} .$$

Ora abbiamo

$$(\varepsilon, x_0) = \sum_r \varepsilon^r x_r ,$$

percorrendo r un sistema completo di resti (mod n) e la coniugata di (ε, x_0) è dunque

$$\sum_r \varepsilon^{-r} x_{r+\frac{n}{2}} .$$

Ponendo $r + \frac{n}{2} = \rho$ ed osservando che ρ percorre con r un sistema completo di resti (mod n), la quantità precedente può scriversi

$$\sum_\rho \varepsilon^{-\rho+\frac{n}{2}} x_\rho$$

---

[1]) Cf. Weber. — Bd. I, p. 548.

e a causa di $\varepsilon^{\frac{n}{2}} = -1$ si ha

$$\sum_{\rho} \varepsilon^{-\rho+\frac{n}{2}} x_\rho = -\sum_{\rho} \varepsilon^{-\rho} x_\rho = -(\varepsilon^{-1}, x_0),$$

ciò che dimostra la nostra asserzione.

La quantità

$$\sqrt[n]{B_1} \sqrt[n]{B_{n-1}} = c_{n-1},$$

che è razionalmente nota (§. 75), è adunque reale e più precisamente positiva o negativa secondo che l'equazione ha le radici reali od immaginarie. Se poniamo la quantità razionalmente nota B_1 sotto la forma

$$B_1 = \rho (\cos \omega + i \operatorname{sen} \omega)$$

sarà, per quanto sopra abbiamo visto,

$$B_{n-1} = \rho (\cos \omega - i \operatorname{sen} \omega),$$

indi

$$B_1 B_{n-1} = \rho^2 = c^n,$$

avendo indicato con c il valore assoluto di c_{n-1}. Ne deduciamo

$$\sqrt[n]{\rho} = \sqrt{c}$$

e quindi

$$\sqrt[n]{B_1} = \sqrt{c} \left(\cos \frac{\omega + 2r\pi}{n} + i \operatorname{sen} \frac{\omega + 2r\pi}{n} \right).$$

La c stessa, come le altre c_i che figurano nella formola (B) di risoluzione, sono razionalmente esprimibili per

$$\varepsilon = \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n},$$

onde alla (B) si potrà dare la forma

$$x_0 = \frac{1}{n} \Big\{ -a_1 + \sqrt{c} \left(\cos \frac{\omega + 2r\pi}{n} + i \operatorname{sen} \frac{\omega + 2r\pi}{n} \right) +$$

$$+ (\alpha + i\beta) \left(\cos \frac{2(\omega + 2r\pi)}{n} + i \operatorname{sen} \frac{2(\omega + 2r\pi)}{n} \right)$$

$$(\alpha' + i\beta') \sqrt{c} \left(\cos \frac{3(\omega + 2r\pi)}{n} + i \operatorname{sen} \frac{3(\omega + 2r\pi)}{n} \right) + \ldots \Big\},$$

essendo c, α, β, α', β' ... quantità razionali in $\cos\frac{2\pi}{n}$, $\operatorname{sen}\frac{2\pi}{n}$. Possiamo quindi enunciare il risultato sotto forma geometrica:

Per risolvere in un campo di razionalità reale un' equazione Abeliana ciclica di grado n basta eseguire le operazioni seguenti:

1.ª *dividere la circonferenza in n parti eguali;*

2.ª *dividere un angolo* ω, *che si può costruire, in n parti eguali;*

3.ª *estrarre la radice quadrata da un' unica quantità c.*

Si osserverà che, se n è una potenza esatta del 2, tutte le costruzioni geometriche qui indicate sono eseguibili elementarmente cioè col solo uso della riga e del compasso.

§. 78. — Per ricercare le condizioni di risolubilità per radicali di un' equazione è necessario che consideriamo più da vicino quella prima e più semplice classe di equazioni Abeliane alle quali conduce il problema della divisione della circonferenza in un numero qualunque di parti eguali. Esporremo più tardi (Cap. VII) la teoria di queste equazioni, dovuta a Gauss, che primo ne dimostrò la risolubilità per radicali; ma per ora ci limiteremo ad esporre quanto è necessario conoscere per l' accennata ricerca.

Se p è un numero primo, l' equazione

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

ha per radici le $p-1$ radici primitive dell' unità

$$c^{\frac{2r\pi i}{p}} = \cos\frac{r.2\pi}{p} + i \operatorname{sen}\frac{r.2\pi}{p}$$
$$r = 1, 2, 3 \ldots p-1,$$

e la risoluzione di questa equazione equivale appunto geometricamente alla iscrizione nel cerchio del poligono regolare di p lati. Importa che determiniamo, nel campo assoluto di razionalità, il gruppo di Galois per questa equazione. A tale oggetto cominciamo dal dimostrare il teorema:

L'equazione: $x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$ *alle radici primitive* p^{me} *dell'unità è irriducibile.*

Ciò segue facilmente dal teorema dimostrato al principio del §. 60 (Eisenstein).

Posto infatti $x=y+1$, la nostra equazione diventa

$$\frac{(y+1)^p-1}{y}=0,$$

ossia

$$y^{p-1}+py^{p-2}+\frac{p(p-1)}{2}y^{p-3}+\ldots+p=0$$

ed avendo tutti i coefficienti, dopo il primo, divisibili per p e l'ultimo $=p$, essa è certamente irriducibile.

Ora se poniamo

$$\varepsilon=e^{\frac{2\pi i}{p}},$$

tutte le altre radici sono esprimibili razionalmente per ε; inoltre possiamo ordinarle in guisa che formino un unico periodo. Indicando infatti con g una radice primitiva (mod p), le $p-1$ radici

$$\varepsilon,\ \varepsilon^g,\ \varepsilon^{g^2}\ldots\varepsilon^{g^{p-2}}$$

sono distinte fra loro perchè si ha $\varepsilon^r=\varepsilon^s$ solo quando $r\equiv s$ (mod p), e ciascuna di esse è la potenza g^{ma} della precedente, mentre

$$(\varepsilon^{g^{p-2}})^g=\varepsilon^{g^{p-1}}=\varepsilon.$$

Per quanto abbiamo visto al §. 74, risulta che il gruppo di Galois della nostra equazione è il gruppo ciclico Γ_{p-1} generato dalle $p-1$ potenze della sostituzione

$$S=(\varepsilon,\ \varepsilon^g,\ \varepsilon^{g^2}\ldots\varepsilon^{g^{p-2}}).$$

L'attuale equazione Abeliana è composta e se decomponiamo il grado $p-1$ nei suoi fattori primi, sia

$$p-1=2^\alpha p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r},$$

ed applichiamo le osservazioni al principio del §. 74, abbiamo il teorema seguente:

Per trovare la radice primitiva p^{ma} dell'unità

$$\varepsilon=\cos\frac{2\pi}{p}+i\,\mathrm{sen}\frac{2\pi}{p},$$

essendo p un numero primo e

$$p - 1 = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

basta conoscere le radici primitive dell'unità

$$\varepsilon_1, \varepsilon_2, \ldots \varepsilon_r$$

dei rispettivi ordini

$$p_1, p_2, \ldots p_r,$$

indi estrarre α radici quadrate, α_1 radicali d'indice p_1, α_2 d'indice p_2 ecc.

§. 79. — Dopo le ricerche dei §§. precedenti sulle equazioni Abeliane, riprendiamo la trattazione della teoria generale per completare i risultati, ottenuti al §. 72, sulla riduzione di un'equazione composta a successive equazioni semplici. Tale riduzione è stata ottenuta adoperando delle equazioni ausiliarie semplici speciali e precisamente delle *risolventi* della proposta.

La prima questione da risolversi, per elevarsi alla teoria generale, è ora quella di esaminare se l'abbassamento del gruppo di una equazione può ottenersi aggiungendo al campo di razionalità le radici di un'equazione ausiliaria qualsiasi. Stabiliremo per ciò il seguente teorema fondamentale di Jordan, nel modo come fu completato da Hölder [1]):

Se il gruppo G *di* Galois *per una equazione*

$$f(x) = 0$$

si riduce ad un suo sottogruppo G_1 *per l'aggiunta di tutte le radici di un'equazione ausiliaria*

$$\varphi(y) = 0,$$

viceversa il gruppo Γ *di questa si ridurrà, per l'aggiunta di tutte le radici della primitiva, ad un suo sottogruppo* Γ_1; *inoltre* G_1 *sarà invariante in* G *come* Γ_1 *invariante in* Γ, *e i gruppi complementari*

$$\frac{G}{G_1}, \frac{\Gamma}{\Gamma_1}$$

saranno identici (oloedricamente isomorfi).

---

[1]) Jordan. *Traité des substitutions,* pag. 269. — Hölder. *Mathem. Annalen,* Bd. 34.

Sieno n, m i rispettivi gradi di $f(x)=0$, $\varphi(y)=0$ e

$$x_1, x_2 \ldots x_n$$

$$y_1, y_2 \ldots y_m$$

le loro radici. Indichiamo poi con r l'ordine di G, con r_1 quello del sottogruppo G_1 e con ρ quello di Γ. Costruiamo una funzione razionale

$$z_1 = \psi(x_1 x_2 \ldots x_n)$$

delle radici della proposta, il cui sottogruppo numerico sia precisamente G_1 (§. 69), e con essa costruiamo una risolvente

$$\Theta(z) = 0$$

della proposta, che avrà per grado $\frac{r}{r_1}$ e per gruppo il gruppo complementare $\frac{G}{G_1}$. Se al campo attuale di razionalità aggiungiamo le radici

$$y_1 y_2 \ldots y_m$$

dell'ausiliaria $\varphi(y)=0$, il gruppo G della proposta scende, per ipotesi, a G_1 e però z_1 è esprimibile razionalmente per $y_1, y_2, \ldots y_m$, poniamo

$$z_1 = \psi(x_1, x_2 \ldots x_n) = \Phi(y_1 y_2 \ldots y_m).$$

Indichiamo ora con Γ_1 il sottogruppo numerico di Γ per la funzione $\Phi(y_1 y_2 \ldots y_m)$ e formiamo con questa funzione Φ la corrispondente risolvente di $\varphi(y)=0$, che avrà per ordine $\frac{\rho}{\rho_1}$, essendo ρ_1 l'ordine di Γ_1, e avrà per gruppo $\frac{\Gamma}{\Gamma_1}$. Ma questa risolvente, irriducibile come la $\Theta(z)=0$, avendo con essa a comune la radice

$$\Psi(x_1 x_2 \ldots x_n) = \Phi(y_1 y_2 \ldots y_n),$$

coincide necessariamente con $\Theta(z)=0$ e si ha quindi intanto

$$\frac{r}{r_1} = \frac{\rho}{\rho_1}, \quad \frac{G}{G_1} = \frac{\Gamma}{\Gamma_1}.$$

Se indichiamo ora con

$$z_1, z_2 \ldots z_q$$

le $q = \frac{r}{r_1}$ radici della risolvente comune $\Theta(z)=0$ di $f(x)=0$, $\varphi(y)=0$,

aggiunte al campo di razionalità $y_1 y_2 \ldots y_m$ è nota non soltanto la prima radice z_1 di $\Theta(z) = 0$ ma anche tutte le altre, essendo tutte funzioni razionali delle y. Dunque, considerate come funzioni delle x, le

$$z_1, z_2 \ldots z_q$$

hanno tutte il medesimo sottogruppo numerico G_1, dovendo tutte rimanere invariate per le sostituzioni di G_1, che è per ipotesi il gruppo di Galois di $f(x) = 0$ dopo l'aggiunta di $y_1 y_2 \ldots y_m$. Ne segue che G_1 è invariante in G e $z_2 z_3 \ldots z_q$ sono funzioni razionali di z_1, cioè la risolvente $\Theta(z) = 0$ è un'equazione normale.

Osserviamo ora come si abbassa il gruppo Γ della $\varphi(y) = 0$, aggiungendo al campo di razionalità le radici

$$x_1, x_2 \ldots x_n,$$

della primitiva. Siccome

$$z_1 = \Phi(y_1 y_2 \ldots y_m) = \Psi(x_1 x_2 \ldots x_n),$$

dopo tale aggiunta, viene ad essere razionalmente nota, il gruppo Γ si abbasserà certamente o a Γ_1 o ad un sottogruppo di Γ_1. Ma l'ultima ipotesi facilmente si esclude, poichè intanto le nostre considerazioni dimostrano che per l'indice q' del sottogruppo Γ_2 di Γ a cui Γ si abbassa per l'aggiunta di tutte le radici di $f(x) = 0$ si ha

$$q' \geq q,$$

essendo q l'indice del sottogruppo G_1 del gruppo G di $f(x) = 0$, a cui si abbassa G per l'aggiunta delle radici di $\varphi(y) = 0$. Ma allora, se scambiamo in questo risultato le due equazioni $f(x) = 0$, $\varphi(y) = 0$, troviamo anche

$$q \geq q'$$

e per ciò $q' = q$ e $\Gamma_2 = \Gamma_1$ c. d. d. Naturalmente poi è Γ_1 invariante in Γ come G_1 in G e il nostro teorema è completamente dimostrato.

Come corollario del teorema fondamentale, notiamo che, se l'equazione ausiliaria $\varphi(y) = 0$ è semplice, sarà $\Gamma_1 = 1$ e quindi ogni sua radice sarà nota quando si aggiungano al campo di razionalità $x_1, x_2 \ldots x_n$. Dunque:

Ogni equazione ausiliaria semplice, la cui risoluzione contribuisca all'abbassamento del gruppo della proposta, è necessariamante una risolvente di questa.

D'altra parte, col teorema al §. 72, possiamo sempre sostituire ad ogni equazione ausiliaria composta una successione di equazioni ausiliarie semplici, che saranno quindi risolventi della primitiva. Vediamo dunque che la generalizzazione introdotta nelle ricerche primitive del §. 72, col considerare equazioni ausiliarie qualunque invece di risolventi, è in fondo soltanto apparente e il teorema del §. 72 ci dà tutto ciò che si può conseguire, per la risoluzione di un'equazione, per mezzo di successive equazioni ausiliarie.

In fine osserviamo che se la proposta è alla sua volta un'equazione semplice, qualunque ausiliaria semplice, la cui risoluzione contribuisca all'abbassamento del gruppo della primitiva e lo riduca quindi, G essendo semplice, all'identità, ha il medesimo gruppo Γ della primitiva (oloedricamente isomorfo).

§. 80. — Siamo ora in grado di ricercare le condizioni di *risolubilità per radicali* di un'equazione $f(x) = 0$.

Supponiamo per ciò dapprima che i fattori di composizione

$$p_1, p_2 \cdots p_r$$

del gruppo G di $f(x) = 0$ siano tutti numeri primi e dimostriamo che allora l'equazione sarà risolubile per radicali. Per ciò, applicando il teorema generale al §. 72, vediamo in primo luogo che le successive equazioni ausiliarie semplici (risolventi):

$$\varphi_{p_1}(y) = 0 \ , \ \varphi_{p_2}(z) = 0 \ldots$$

sono equazioni Abeliane di grado primo a gruppo ciclico e però risolubili con rispettive estrazioni di radicali d'indici $p_1, p_2 \ldots p_r$ e coll'aggiunta delle corrispondenti radici dell'unità

$$\varepsilon_1, \ \varepsilon_2 \ldots \varepsilon_r$$

d'ordini $p_1, p_2 \ldots p_r$. Dunque:

Se il gruppo G *di un'equazione ha per fattori di composizione altrettanti numeri primi*

$$p_1, p_2 \cdots p_r,$$

l'equazione si risolve estraendo successivi radicali d'indici eguali a questi fattori primi [1]).

Ora ci proponiamo di dimostrare inversamente che, se un'equazione $f(x)=0$ è risolubile per radicali, i fattori di composizione del suo gruppo dovranno essere altrettanti numeri primi. Noi supponiamo adunque che le radici di $f(x)=0$ possano esprimersi per mezzo di successive estrazioni di radicali da effettuarsi sopra quantità note o che tali diventano dopo l'aggiunta di radicali precedenti. Aggiungendo via via i varii radicali che si presentano nella supposta formola di risoluzione, nell'ordine stesso che dovrebbe tenersi per l'effettivo calcolo numerico, da ultimo il gruppo della equazione proposta dovrà trovarsi ridotto all'identità, l'equazione essendo risoluta.

Ora estrarre un radicale d'indice composto equivale ad estrarre successivi radicali d'indice primo e quindi possiamo dire che il gruppo di $f(x)=0$ dovrà ridursi all'identità aggiungendo successivamente le radici di equazioni ausiliarie binomie della forma

$$(\alpha) \qquad z^p = A,$$

dove p è un numero primo ed A una quantità nota, o razionalmente esprimibile per quelle aggiunte prima.

Indicando con z_1 una radice della (α), saranno

$$z_1,\ z_2 = \varepsilon z_1,\ z_3 = \varepsilon^2 z_1, \ldots z_{p-1} = \varepsilon^{p-1} z_1$$

$$\varepsilon = e^{\frac{2\pi i}{p}}$$

le altre radici sicchè, ampliato il campo coll'aggiunta di ε, la (α) è una equazione Abeliana. Se la supponiamo riducibile, essa, come equazione normale, dovrà scindersi in fattori iriducibili di egual grado r (§. 63) e per ciò, essendo r un divisore puro del numero primo p, sarà $r=1$. Allora tutte le radici della (α) saranno razionali in (α) e l'aggiunta del radicale $\sqrt[p]{A}$ potrà omettersi come superflua [2]). Supposto che ciò non

---

[1]) Sottintendiamo che siano aggiunte le corrispondenti radici $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_r$ dell'unità, come è necessario per dare ai radicali tutti i loro valori.

[2]) Della proprietà dedotta nel testo dal fatto che la (α) è un'equazione normale di grado primo diamo qui la dimostrazione diretta seguente. Siano $z_1, z_2 \ldots z_\nu$ le radici di un fattore irriducibile della (α) dove dunque $\nu < p$. Il loro prodotto

accada, il gruppo della (α) è dunque un gruppo ciclico Γ_p sulle p radici ed applicando il teorema fondamentale del §. 79, troviamo quindi il risultato:

a) Se, aggiunta la radice p^{ma} dell'unità ε, il gruppo della proposta è G *e, per la successiva aggiunta di un radicale d'indice p: $\sqrt[p]{A}$, il gruppo* G *si abbassa, esso si ridurrà ad un suo sottogruppo invariante* G_1 *d'indice $= p$.*

Resta ora che vediamo quale abbassamento può aver prodotto nel primitivo gruppo dell'equazione l'aggiunta della radice p^{ma} dell'unità e per ciò dimostreremo il teorema:

b) Se il gruppo G′ *della proposta in un primitivo campo di razionalità* (R, R′, R″ . . .) *scende ad un suo sottogruppo* G, *per la successiva aggiunta della radice p^{ma} ε dell'unità, sarà* G *invariante in* G′ *e fra* G′, G *potrà inscrirsi una serie di sottogruppi*

$$G', \; H, \; H_1, \; H_2 \ldots G,$$

tali che ciascuno sia invariante nel precedente ed abbia per indice un numero primo.

E invero, aggiungendo ε, noi aggiungiamo tutte le radici dell'equazione Abeliana

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0,$$

il cui gruppo Γ″ nel campo (R, R′ . . .) sarà o il gruppo ciclico Γ_{p-1} dell'equazione stessa nel campo assoluto di razionalità (§. 78), ovvero un suo sottogruppo. Dunque G è certamente invariante in G′ ed esiste, pel teorema fondamentale §. 79, in Γ″ un sottogruppo invariante Γ tale che i gruppi complementari $\frac{G'}{G}$, $\frac{\Gamma'}{\Gamma}$ sono oloedricamente isomorfi. Ma, essendo Γ″ un gruppo Abeliano e Γ un suo sottogruppo, è certo possibile

---

$z_1 z_2 \ldots z_\nu$ sarà una quantità K razionalmente nota, onde avremo un'eguaglianza della forma

$$\varepsilon^r z_1^\nu = K.$$

Risolvasi ora in numeri interi α, β l'equazione $p\alpha + \nu\beta = 1$ ed elevando la precedente eguaglianza alla potenza β, osservando che $z_1^p = A$ si troverà

$$z_1 = A^\alpha \; K^\beta \; \varepsilon^{-r\beta}$$

onde $z_1, z_2 \ldots z_p$ sono razionali in ε c. d. d.

(§§. 30-33) inserire fra Γ', Γ una serie di sottogruppi i cui fattori di composizione siano numeri primi; la stessa cosa è dunque possibile anche fra G' e G.

§. 81. — Basta ora riunire i risultati del §. precedente per ottenere il teorema finale:

Affinchè un'equazione sia risolubile per radicali è necessario e sufficiente che tutti i fattori di composizione del suo gruppo siano numeri primi.

È per questa ragione appunto che si dà il nome di gruppi *risolubili* a quei gruppi che hanno fattori di composizione primi (§. 27).

Come abbiamo visto al §. 68, l'equazione generale di grado n ha per gruppo il gruppo totale $G_{\pi(n)}$. Ora i fattori di composizione di questo gruppo, appena $n > 4$, sono:

$$2\ ,\ \frac{1}{2}\,\pi\,(n) \quad (\S.\ 24)\ ,$$

onde concludiamo:

Le equazioni generali di grado superiore al quarto non sono risolubili per radicali.

Ciò vale in particolare della equazione generale di 5.° grado, come pei primi dimostrarono Ruffini ed Abel [1]).

L'unico abbassamento possibile nel gruppo dell'equazione generale di grado n è quello che si ottiene aggiungendo al campo di razionalità la radice quadrata del discriminante

$$\Delta = \prod_{r,s} (x_r - x_s)^2.$$

Siccome $\sqrt{\Delta}$ è una funzione invariabile per le sostituzioni pari, la sua aggiunta abbassa il gruppo dell'equazione al gruppo alterno $G_{\frac{\pi(n)}{2}}$, dopo di che sono razionalmente note non solo le funzioni simmetriche delle radici, ma anche le *semisimmetriche*, cioè quelle invariabili per le sostituzioni del gruppo alterno, che possono esprimersi tutte sotto la forma

$$A + B\sqrt{\Delta}\ ,$$

[1]) Sebbene le dimostrazioni date da Ruffini non possano considerarsi come completamente rigorose, è tuttavia negli scritti del geometra italiano che la questione viene per la prima volta posta e trattata. Ivi si trovano altresì i primi germi della teoria dei gruppi di sostituzioni, sviluppata poi da Cauchy e da Galois.

essendo A, B razionali nei coefficienti della equazione. Ma, il gruppo alterno essendo semplice, qualunque ulteriore abbassamento è impossibile non solo per estrazioni di radicali ma anche per aggiunta di radici di equazioni ausiliarie.

Come si è visto al §. 68, non solo le equazioni generali di grado n ma persino equazioni a coefficienti numerici hanno, nel campo assoluto di razionalità, per gruppo di Galois il gruppo totale e non sono quindi risolubili per radicali. Tale è per esempio l'equazione di 5.° grado (§. 68)

$$x^5 + px^2 - px - p = 0$$

con p numero primo.

Se applichiamo i teoremi ottenuti alle equazioni generali di grado $n = 2, 3, 4$, chiaramente vediamo a quali circostanze è dovuta la loro risolubilità per radicali.

Per $n = 2$ l'aggiunta della radice quadrata del discriminante abbassa il gruppo all'identità (gruppo alterno) e risolve quindi l'equazione.

Per $n = 3$ abbiamo la serie di composizione

G_6	G_3	1
gruppo totale	gruppo alterno	identità

coi fattori di composizione 2. 3. L'estrazione della radice quadrata del discriminante abbassa il gruppo al gruppo ciclico G_3 e l'equazione, che diventa allora Abeliana, si risolve estraendo un radicale cubico.

Per $n = 4$ la serie di composizione è

G_{24}	G_{12}	G_4	G_2	1
gruppo totale	gruppo alterno	(Vierergruppe)		

coi fattori di composizione

$$2, 3, 2, 2 .$$

L'estrazione di una prima radice quadrata (sul discriminante) abbassa il gruppo a G_{12}, quella di un radicale cubico a G_4 e l'equazione diventa allora Abeliana cogli invarianti [2, 2] e la successiva estrazione di due radici quadrate separate (§. 76) risolve l'equazione.

Si potrebbe anche vedere come, applicando il teorema generale del §. 72 alle equazioni di 3.° e 4.° grado, si ottengono le ordinarie formole di risoluzione.

§. 82. — Le ricerche precedenti sono relative alla *completa risolubilità* per radicali di una equazione. Si potrebbe per altro pensare che esistessero equazioni *irriducibili* di cui una o più radici si potessero esprimere per radicali, senza che ciò fosse possibile per tutte. È ben naturale che per equazioni riducibili questo è possibile; ma nel caso della irriducibilità possiamo dimostrare il teorema:

Un'equazione irriducibile, di cui una o più radici possano esprimersi per radicali, è totalmente risolubile per radicali.

Nelle memorie di Abel questa proprietà è enunciata dicendo che se ad una equazione irriducibile si può soddisfare algebricamente (con espressioni contenenti solo radicali) essa è risolubile algebricamente (per radicali).

Supponiamo adunque che, per successive estrazioni di radicali, si pervenga a conoscere una o più radici di una equazione irriducibile di grado n e, come al §. 80, seguiamo via via l'abbassamento prodotto nel gruppo della equazione per queste successive aggiunte. Il gruppo della equazione, che era primitivamente transitivo, sarà certo diventato intransitivo quando le aggiunte dei successivi radicali avranno resa razionalmente nota una radice. Poniamo che il primo abbassamento da un gruppo transitivo G ad uno intransitivo G_1 abbia luogo per l'aggiunta di un radicale d'indice primo p, sia $\sqrt[p]{A}$ [1]). Pel teorema *a*) al §. 80 sarà G_1 invariante d'indice p in G e poichè G_1 è intransitivo, G invece transitivo, i sistemi di transitività in cui si scindono le n radici rispetto a G_1 conterranno tutti un egual numero r di lettere, come si vede ripetendo un ragionamento che abbiamo fatto al principio del §. 35 pel gruppo metaciclico. Dunque intanto, se il grado n della nostra equazione è un numero primo, sarà $r = 1$, cioè tutte le radici saranno note e l'equazione sarà dunque totalmente risolubile per radicali, come porta l'enunciato del teorema.

In generale se

$$(x_1\, x_2 \ldots x_r)\ ,\ (x_{r+1}\, x_{r+2} \ldots x_{2r}) \ldots$$

---

[1]) Nessun altro caso è da considerare perchè l'aggiunta della radice p^{ma} dell'unità si riduce, pel teorema alla fine del §. 68, a successive aggiunte di radicali d'indice primo.

sono i sistemi di transitività, saranno

$$\varphi_1(x, \sqrt[p]{A}) = (x - x_1)(x - x_2)\dots(x - x_r)$$

$$\varphi_2(x, \sqrt[p]{A}) = (x - x_{r+1})(x - x_{r+2})\dots(x - x_{2r})$$

. . . . . .

i nuovi fattori irriducibili di $f(x)$ nel campo ampliato coll'aggiunta di $\sqrt[p]{A}$.

Le sostituzioni di G_1 sono ciascuna il prodotto di sostituzioni di varii gruppi parziali

$$\Gamma_1, \Gamma_2, \Gamma_3 \dots$$

operanti transitivamente sulle lettere dei singoli sistemi. Questi gruppi $\Gamma_1, \Gamma_2, \Gamma_3 \dots$ sono i rispettivi gruppi di Galois per le equazioni

$$\varphi_1(x, \sqrt[p]{A}) = 0, \quad \varphi_2(x, \sqrt[p]{A}) = 0, \quad \varphi_3(x, \sqrt[p]{A}) = 0 \dots$$

Ora, siccome G_1 è invariante nel gruppo transitivo G, si vede subito che $\Gamma_1, \Gamma_2, \Gamma_3 \dots$ sono fra loro oloedricamente isomorfi e quindi se l'equazione

$$\varphi_1(x, \sqrt[p]{A}) = 0$$

è risolubile per radicali, tali saranno pure le altre. Ma questa equazione ha, per ipotesi, una radice x_1 esprimibile per radicali, talchè il teorema enunciato è certamente vero per le equazioni di grado n se lo è per le equazioni di grado inferiore, divisore di n. Ed, essendo dimostrato per le equazioni di grado primo, sarà dunque vero in generale c. d. d.

§. 83. — Nelle ricerche fondamentali del §. 79 abbiamo esaminato l'abbassamento che può prodursi nel gruppo di un'equazione $f(x) = 0$ per l'aggiunta di *tutte* le radici di un'equazione ausiliaria $\varphi(y) = 0$. Qui vogliamo generalizzare la ricerca ed esaminare ciò che accade quando si aggiunga *una* radice di un'equazione ausiliaria. Ci limiteremo per altro al caso, che basta al nostro scopo, in cui *l'equazione ausiliaria sia irriducibile e di grado primo*. Siccome poi al problema di risolvere un'equazione $f(x) = 0$ si può sostituire quello relativo alla sua risolvente di Galois, che è un'equazione normale, potremo supporre che la $f(x) = 0$ stessa sia un'equazione normale, senza limitare ulteriormente la nostra ricerca.

Ciò posto, supponiamo che per l'aggiunta di *una* radice y_1 dell'ausiliaria irriducibile

$$\varphi_p(y) = 0$$

di grado primo p, il gruppo di GALOIS G della equazione normale

$$f(x) = 0$$

scenda al sottogruppo G_1 e indichiamo con

$$x_1 x_2 \ldots x_n$$

le radici della proposta e con

$$y_1 y_2 \ldots y_p$$

quelle dell'ausiliaria. Prendiamo una funzione razionale $\psi(x_1 x_2 \ldots x_n)$ delle x a sottogruppo numerico $= G_1$, che, per essere la $f(x) = 0$ una equazione normale, si potrà anche esprimere razionalmente per la sola x_1, sia

$$\psi(x_1 x_2 \ldots x_n) = \Phi(x_1).$$

La $\Phi(x_1)$ sarà nota dopo l'aggiunta di y_1 e si avrà quindi

$$\Phi(x_1) = \Theta(y_1),$$

essendo Θ razionale intera di grado $p-1$ al massimo. Se colla funzione $\Phi(x_1)$ costruiamo la risolvente della proposta

$$(\beta) \qquad F_q(\Phi) = 0,$$

il cui grado q eguaglierà l'indice di G_1 in G, avremo

$$F_q(\Theta(y_1)) = 0,$$

onde per l'irriducibilità della $\varphi_p(y) = 0$ segue che i p valori

$$(\gamma) \qquad \Theta(y_1)\ \Theta(y_2) \ldots \Theta(y_p)$$

sono tutte radici della (β). Questi p valori (γ) sono tutti distinti fra loro poichè, se fosse p. e.

$$\Theta(y_1) = \Theta(y_2) = \ldots = \Theta(y_r) \quad r > 1,$$

applicando a queste relazioni le sostituzioni del gruppo *transitivo* di GALOIS della $\varphi(y) = 0$ ne dedurremmo che le p quantità (γ) sono r ad r eguali quindi $r = p$ e $\Theta(y_1) = \Phi(x_1)$ sarebbe allora razionalmente nota nel

campo primitivo. Ora dalla (β) si separa il fattore evidentemente razionale

$$(\Phi - \Theta(y_1))\,(\Phi - \Theta(y_2))\ldots(\Phi - \Theta(y_p)) = 0$$

e quindi, per l'irriducibilità della risolvente (β), avremo

$$q = p\,.$$

Ora se per l'equazione $\varphi_p(y) = 0$ aggiungiamo al campo di razionalità x_1, tutte le radici (γ) della (β) sono razionalmente note e siccome la sola sostituzione identica sulle y lascia invariate le (γ) vediamo che, dopo l'aggiunta di x_1, il gruppo di $\varphi_p(y) = 0$ si riduce all'identità, onde segue che le y sono funzioni razionali delle x quindi di x_1 e la $\varphi_p(y) = 0$ non è che una risolvente della proposta. Abbiamo dunque il teorema:

Se per l'aggiunta di una radice di un'equazione ausiliaria irriducibile di grado primo p il gruppo di un'equazione $f(x) = 0$ scende da G *a* G_1, *sarà* G_1 *sottogruppo (in generale non invariante) d'indice p in* G *e l'equazione ausiliaria non sarà altro che una ordinaria risolvente di $f(x) = 0$, costruita con una funzione razionale y_1 delle radici della proposta invariabile numericamente pel sottogruppo* G_1.

Supponiamo ora che il campo di razionalità sia reale e l'equazione

$$f(x) = 0$$

abbia tutte le radici reali. Allora ogni ausiliaria irriducibile $\varphi_p(y) = 0$ di grado primo p, di cui la conoscenza di una radice abbassi il gruppo di $f(x) = 0$, come risolvente della proposta in un campo reale, avrà essa stessa tutte le radici reali. Abbiamo dunque il teorema:

Se, per l'aggiunta di una radice di una equazione ausiliaria irriducibile di grado primo, il gruppo di una equazione a radici reali in un campo reale di razionalità viene abbassato, anche l'ausiliaria avrà certamente tutte le radici reali.

§. 84. — Il risultato ora ottenuto consente un'applicazione molto notevole al caso in cui si voglia abbassare il gruppo di un'equazione in un campo reale di razionalità, ampliando il campo coll'aggiunta di radicali *reali*

$$\sqrt[p]{A}\,,$$

dove A è una quantità reale appartenente al campo di razionalità.

Siccome l'equazione binomia

$$z^p = A$$

è irriducibile, come si è visto al §. 80, a meno che non sia A una potenza p^{ma} esatta (nel qual caso l'aggiunta di $\sqrt[p]{A}$ non amplierebbe il campo di razionalità) e siccome d'altra parte una sola sua radice è reale, salvo quando $p = 2$ ed A è positivo, vediamo che:

Se un'equazione $f(x) = 0$ ha coefficienti e radici tutte reali e G è il suo gruppo in un campo reale di razionalità, l'aggiunta di quanti si vogliano radicali reali non può mai abbassare il gruppo, a meno che ciò accada per estrazione di radici quadrate su quantità positive.

Si aggiunga che nel caso in cui l'aggiunta di un radicale quadrato $\sqrt{A}$ abbasso il gruppo, questo scenderà ad un suo sottogruppo (invariante) d'indice 2. Ciò resta naturalmente impossibile se l'ordine del gruppo non è divisibile per 2. Così per un'equazione Abeliana di grado impari in un campo reale di razionalità, tutte le radici essendo reali e l'ordine del gruppo eguale al grado (impari) dell'equazione, è impossibile qualunque abbassamento del gruppo per radicali reali. L'equazione è bensì risolubile per radicali; ma questi portano necessariamente gli immaginarii e, volendoli ridurre a forma reale, si può unicamente ricorrere alla divisione di un angolo noto in n parti eguali, secondo il teorema d'Abel al §. 77.

Un caso particolare è quello dell'equazione cubica, che possiamo ridurre alla forma

$$x^3 + px + q = 0.$$

Nella formola Cardanica di risoluzione

$$x = \sqrt[3]{-\frac{p}{2} + \sqrt{\frac{p^2}{4} + \frac{q^3}{27}}} + \sqrt[3]{-\frac{p}{2} - \sqrt{\frac{p^2}{2} + \frac{q^3}{27}}},$$

quando le tre radici sono reali, si presenta il così detto *caso irriducibile.* Allora si ha che il discriminante

$$\Delta = -4 \,.\, 27 \left(\frac{p^2}{4} + \frac{q^3}{27}\right)$$

è positivo e l'estrazione di radice cubica porta su quantità immaginarie. Ogni tentativo di ricondurre la formola a radicali reali, senza ricorrere

alle formole trigometriche (trisezione dell'angolo) riporta alla equazione medesima. I risultati generali ottenuti ci fanno comprendere la necessità di questo fatto. E invero l'equazione cubica, appena aggiunto il radicale quadrato $\sqrt{\Delta}$, che è nel caso attualmente considerato reale, acquista per gruppo il gruppo alterno G_3 e diventa quindi, nel campo reale $(p, q, \sqrt{\Delta})$, un'equazione Abeliana di grado impari 3. Nessuna estrazione di radicali reali può ulteriormente abbassare il gruppo.

§. 85. — Ritorniamo alle equazioni di grado n, a gruppo totale $G_{\pi(n)}$, per trattare la seguente questione che ha molto occupato i matematici:

Può un'equazione generale di grado n possedere risolventi di grado minore od eguale a n?

Per quanto sappiamo intorno alla formazione delle risolventi, il problema enunciato equivale all'altro

Esistono nel gruppo totale $G_{\pi(n)}$ *sottogruppi d'indice* $\leq n$? Un'altra forma della medesima questione consiste nel ricercare le funzioni razionali di n variabili $x_1, x_2 \ldots x_n$ che abbiano n o meno di n valori distinti.

Sia Γ un sottogruppo d'indice $r \leq n$ e formiamo la risolvente con una funzione razionale delle radici della proposta numericamente invariabile per le sostituzioni di Γ. Indicando con

$$y_1, y_2, \ldots y_r$$

le radici di questa risolvente, il suo gruppo sarà il gruppo complementare $H = \frac{G}{\Gamma}$ col quale G sarà isomorfo; all'identità in H corrisponderà un sottogruppo Σ *invariante* in $G_{\pi(n)}$ (precisamente il sottogruppo comune a Γ e a tutti i sottogruppi affini in $G_{\pi(n)}$), onde, eccettuato il caso $n = 4$, sarà Σ l'identità ovvero il gruppo alterno. Ora, se supponiamo dapprima $r < n$, il primo caso non può darsi perchè l'isomorfismo di G, H sarebbe allora oloedrico, mentre l'ordine di H, divisore di $\pi(r)$, è certo minore di quello $\pi(n)$ di G. Dunque Σ sarà in questo caso il gruppo alterno e per ciò y_1 sarà una funzione semi-simmetrica (a due valori) onde concludiamo:

Un'equazione di grado n, che abbia per gruppo di Galois *il gruppo totale (come l'equazione generale), non possiede altra risolvente di grado* $< n$ *all'infuori di quella di secondo grado* $y^2 = \Delta$, *indicando* Δ *il discriminante. Fa eccezione soltanto il caso* $n = 4$.

Si può osservare di più che anche ridotto, coll'estrazione della radice quadrata di Δ, il gruppo dell'equazione al gruppo alterno, non si può nemmeno costruire, a causa della semplicità di questo gruppo, alcuna risolvente di grado $< n$.

Riferendoci ai gruppi stessi totale ed alterno, possiamo enunciare il risultato dicendo: *Il gruppo totale ed il gruppo alterno sopra $n > 4$ lettere non posseggono alcun sottogruppo d'indice eguale ad uno dei numeri*

$$3,\ 4,\ 5 \ldots n-1 .$$

Il caso $n = 4$ fa realmente eccezione poichè il gruppo totale G_{24} possiede (tre) sottogruppi dell'ottavo ordine e quindi l'equazione generale di 4.° grado ammette una risolvente cubica. Ed è appunto su questa circostanza che si fondano i metodi di risoluzione della equazione del 4.° grado. Così, indicate con

$$x_1,\ x_2,\ x_3,\ x_4$$

le radici dell'equazione generale di 4.° grado

$$(\gamma) \qquad x^4 + a x^3 + b x^2 + e x + d = 0 ,$$

è una funzione a tre valori la seguente

$$y_1 = x_1 x_2 + x_3 x_4 ,$$

il cui gruppo è il gruppo dell' 8.° ordine

$$G_8 = \begin{cases} 1 \ , & (x_1 x_2)(x_3 x_4) \ , & (x_1 x_3)(x_2 x_4) \ , & (x_1 x_4)(x_2 x_3) \\ (x_1 x_2) \ , & (x_3 x_4) \ , & (x_1 x_4 x_2 x_3) \ , & (x_1 x_3 x_2 x_4) \end{cases} .$$

Gli altri due valori di y_1 sono

$$y_2 = x_1 x_3 + x_2 x_4 ,\ y_3 = x_1 x_4 + x_2 x_3$$

e, poichè si trova

$$\sum y_1 = b ,\ \sum y_1 y_2 = a c - 4 d ,\ \sum y_1 y_2 y_3 = c^2 + d (a^2 - 4 b) ,$$

la corrispondente risolvente di 3.° grado si scrive

$$(\delta) \qquad y^3 - b y^2 + (a c - 4 d) y + d (4 b - a^2) - c^2 = 0 .$$

Ne abbiamo notata la forma esplicita per poter stabilire il criterio di risolubilità dell'equazione di 4.° grado *per radicali quadratici*. In tale

ipotesi anche l'equazione cubica dovrà risolversi per radicali quadratici e però dovrà possedere una radice razionale. Se ne conclude: *L'equazione di 4.° grado* (γ) *è risolubile per radicali quadratici solo quando la risolvente cubica* (δ) *possiede una radice razionale* [1]).

Così p. e. se $a = c = 0$, la (γ) è biquadratica e la (δ) possiede la radice razionale $y = b$.

Un'equazione *irriducibile* di 4.° grado che sia risolubile per radicali quadrati potrà avere per gruppo il gruppo G_8 (od un suo affine) ovvero il gruppo G_4 (VIERERGRUPPE): precisamente si presenterà il secondo caso od il primo, secondo che il suo discriminante sarà un quadrato perfetto o no. Se il gruppo è G_4 l'equazione si risolve estraendo due radici quadrate separate; nell'altro caso queste due radici portano ciascuna sopra una terza radice quadrata ($\sqrt{\Delta}$) prima estratta.

---

[1]) Come esempio di applicazione geometrica citiamo il seguente problema elementare: *Date in un piano due rette, supposte per semplicità ortogonali, ed un punto, condurre pel punto una trasversale sulla quale le due rette date stacchino un segmento di lunghezza data.*

Prese le due rette fisse per assi coordinati, siano α, β le coordinate del punto fisso e ξ, η i segmenti che la trasversale domandata stacca sugli assi.

Le equazioni del problema sono:

$$\frac{\alpha}{\xi} + \frac{\beta}{\eta} = 1\,,\ \xi^2 + \eta^2 = l^2\,,$$

essendo l la lunghezza data. Eliminando η, risulta l'equazione di 4.° grado in ξ

$$\xi^4 - 2\alpha\xi^3 + (\alpha^2 + \beta^2 - l^2)\,\xi^2 + 2\alpha l^2 \xi - l^2 \alpha^2 = 0$$

che non è risolubile per radicali quadrati, finchè α, β, l restano arbitrari. Così p. e. se facciamo

$$\alpha = 1\,,\ \beta = 2\,,\ l = 1$$

abbiamo l'equazione

$$\xi^4 - 2\xi^3 + 4\xi^2 + 2\xi - 1 = 0\,,$$

la cui risolvente cubica (δ) è:

$$y^3 - 4y^2 - 16 = 0\,,$$

che non ha radici razionali. Il problema proposto non è quindi risolubile (in generale) colla riga e col compasso. In casi particolari, come quando p. e. $\alpha = \pm\beta$ ecc., il problema diventa solubile elementarmente.

§. 86. — Veniamo ora ad esaminare se un'equazione di grado n, a gruppo totale, può possedere una risolvente di grado n. Intanto ogni trasformata di TSCHIRNHAUS della proposta è appunto una risolvente di grado n; ma, salvo che in questo caso ovvio, dimostriamo: *Un'equazione di grado n a gruppo totale non possiede alcuna risolvente di grado n (che non ne sia una semplice trasformata di* TSCHIRNHAUS). *Soltanto il caso $n = 6$ fa eccezione.*

Che il caso $n = 6$ faccia realmente eccezione si vede subito ricordando che il gruppo lineare totale Γ sopra 6 elementi (§. 39) è di ordine $= 120$ e nel gruppo totale $G_{\pi(6)}$ d'ordine $= 6 . 120$ ha appunto l'indice 6.

Una risolvente dell'equazione di 6.° grado, costruita con una funzione razionale delle sei radici invariabile per le sostituzioni di Γ, è quindi appunto di 6.° grado, senza essere una trasformata di TSCHIRNHAUS della proposta.

Per dimostrare il teorema enunciato, cominciamo dall'osservare che il gruppo H sulle n radici

$$y_1 y_2 \ldots y_n$$

della risolvente dovrà essere, per quanto già si è detto al §. precedente, oloedricamente isomorfo col gruppo totale $G_{\pi(n)}$ sulle n lettere $x_1 x_2 \ldots x_n$; altrimenti la y_1 sarebbe simmetrica o semisimmetrica. Ne segue che H sarà il gruppo totale sulle y.

Se g è una sostituzione qualunque di G ed h la corrispondente in H, avranno g, h eguale periodo; a due sostituzioni simili g, g' di G corrisponderanno due sostituzioni simili h, h' in H, poichè da

$$g' = g_1^{-1} g g_1 ,$$

essendo h_1 la corrispondente di H, segue

$$h' = h_1^{-1} h h_1 .$$

Prendiamo ora in G una trasposizione; dovrà corrispondervi in H una sostituzione a periodo 2, cioè un prodotto di trasposizioni. Supponiamo che ad una determinata trasposizione in G corrisponda un prodotto di r trasposizioni in H, allora, per l'osservazione superiore, ad ogni altra trasposizione in G corrisponderà un prodotto di r trasposizioni in H e viceversa ad ogni prodotto di r trasposizioni in H (con

lettere distinte) una trasposizione in G. Perciò dovrà il numero delle trasposizioni su n lettere, cioè $\frac{n\,(n-1)}{2}$, eguagliare il numero dei prodotti distinti di r trasposizioni, con lettere diverse, su n lettere. Ora quest'ultimo numero è dato da

$$\frac{n\,(n-1)\,(n-2)\ldots(n-2\,r+1)}{1\,.\,2\,.\,3\ldots r\,.\,2^r}\ ^{1)}$$

e però dovremo avere

$$\frac{n\,(n-1)}{2} = \frac{n(n-1)\ldots(n-2\,r+1)}{1\,.\,2\,.\,3\ldots r\,.\,2^r}\,. \tag{5}$$

Dimostriamo ora che, eccettuato il caso $n = 6$, si ha necessariamente $r = 1$. Supposto infatti $r > 1$ la (5) si scrive

$$(n-2)\,(n-3)\ldots(n-2\,r+1) - 2^{r-1}\,\pi\,(r) = 0 \tag{6}$$

Ora, se supponiamo $r > 3$, questa equazione per n non ha soluzioni intere perchè, posto

$$f(x) = (x-2)\,(x-3)\ldots(x-2\,r+1) - 2^{r-1}\,\pi\,(r),$$

si ha

$$f(2\,r) = \pi\,(r)\,\{\,(2r-2)\,(2r-3)\ldots(r+1) - 2^{r-1}\,\} > 0$$

e a più forte ragione $f(n) > 0$ per $n > 2\,r$.

---

[1]) Indicando con $\psi\,(r)$ questo numero ed osservando che, aggiungendo ad un prodotto di $r-1$ trasposizioni una trasposizione, si ottengono tutti i prodotti di r trasposizioni, ripetuti ciascuno r volte, otteniamo:

$$\psi\,(r) = \frac{(n-2\,r+2)\,(n-2\,r+1)}{2\,.\,r}\,.\,\psi(r-1)$$

indi

$$\psi\,(r-1) = \frac{(n-2\,r+4)\,(n-2\,r+3)}{2\,.\,(r-1)}\,\psi\,(r-2)$$

. . . . . .

$$\psi\,(2) = \frac{(n-2)\,(n-3)}{2\,.\,1}\,\psi\,(1)$$

e moltiplicando, coll'osservare che $\psi\,(1) = \frac{n\,(n-1)}{2}$, si ha appunto la formola del testo.

Se poi $n < 2r$ è $f(n) = -2^{r-1}\pi(r) < 0$. D'altronde nemmeno per $r = 2$ vi sono soluzioni intere della (6) [1]) e soltanto per $r = 3$ abbiamo la radice intera $n = 6$. Dunque intanto:

Eccettuato il caso $n = 6$, ad ogni trasposizione in G *dovrà corrispondere una trasposizione in* H.

Se per significare la corrispondenza di due sostituzioni g, h in G, H scriviamo

$$g \sim h$$

e supponiamo che si abbia

$$(x_1 x_2) \sim (y_a y_b)\,, \quad (x_1 x_3) \sim (y_c y_d)\,,$$

avremo

$$(x_1 x_2)(x_1 x_3) = (x_1 x_2 x_3) \sim (y_a y_b)(y_c y_d)$$

e però uno degli indici c, d dovrà eguagliare a ovvero b. Senza alterare la generalità possiamo evidentemente supporre $d = a$ e avremo

$$(x_1 x_2) \sim (y_a y_b)\ , \quad (x_1 x_3) \sim (y_a y_c)\,.$$

Ora ad un'altra trasposizione col primo indice x_1, sia $(x_1 x_r)$, dovrà corrispondere, per la medesima ragione, una trasposizione $(y_i y_k)$ che abbia un indice comune con $(y_a y_b)$ ed uno con $(y_a y_c)$; quindi sarà o della forma $(y_a y_k)$ o dell'altra $(y_b y_c)$. Ma quest'ultimo caso si esclude subito perchè

$$(y_b y_c) = (y_a y_b)(y_a y_c)(y_a y_b) \sim (x_1 x_2)(x_1 x_3)(x_1 x_2) = (x_2 x_3)$$

e però ad ogni trasposizione contenente x_1 dovrà corrispondere una trasposizione contenente y_a. Mutando gli indici alle y, potremo quindi supporre che si abbia

$$(x_1 x_r) \sim (y_1 y_r) \quad r = 2, 3 \ldots n$$

e quindi anche

$$(x_r x_s) = (x_1 x_r)(x_1 x_s)(x_1 x_r) \sim (y_1 y_r)(y_1 y_s)(y_1 y_r) = (y_r y_s)\,.$$

E poichè ogni sostituzione si compone con trasposizioni, ne segue che qualunque sostituzione di H si dedurrà dalla corrispondente di G semplicemente cangiando le lettere x_i nelle corrispondenti y_i. Allora alle

---

[1]) Il caso $r = 2$, o più in generale quello di r pari, può anche escludersi *a priori* perchè il gruppo H avrebbe allora soltanto sostituzioni pari.

$\pi(n-1)$ sostituzioni di H che lasciano ferma y_1 corrispondono le $\pi(n-1)$ sostituzioni di G che lasciano ferma x_1, quindi y_1 è razionalmente esprimibile per x_1, cioè la supposta risolvente non è che una ordinaria trasformata di TSCHIRNHAUS della proposta c. d. d.

Il nostro risultato può anche esprimersi dicendo:

Il gruppo totale su n lettere, per $n \neq 6$, non può porsi in corrispondenza d' isomorfismo oloedrico con se medesimo altrimenti che cangiando la denominazione alle lettere.

Per $n = 6$ esiste un'altra tale corrispondenza essenzialmente diversa.

§. 87. — Abbiamo stabilito al §. 81 il criterio di GALOIS per riconoscere dal gruppo di un'equazione se questa è risolubile per radicali, consistente in questo che i fattori di composizione del gruppo debbono essere numeri primi. Per le equazioni il cui grado è un numero *primo*, GALOIS stesso ha spinto più oltre la ricerca nel modo che ora andiamo ad esporre.

Supponiamo che un'equazione *irriducibile* di grado primo p sia risolubile per radicali. Il suo gruppo, dovendo essere transitivo ed avere per fattori di composizione dei numeri primi, sarà (§. 35) o il gruppo metaciclico

$$G_{p(p-1)}$$

sulle p radici convenientemente ordinate

$$x_0, x_1, x_2 \ldots x_{p-1},$$

ovvero un suo sottogruppo d'ordine $p\delta$, con δ divisore di $p-1$. E siccome nel gruppo metaciclico, e a più forte ragione in un suo sottogruppo $G_{p\delta}$, esiste la sola sostituzione identica che non sposta due determinate radici, ne deduciamo:

Se un'equazione irriducibile di grado primo p è risolubile per radicali, prese due radici qualunque, le altre si esprimeranno razionalmente per queste.

Il teorema si può facilmente invertire colle considerazioni seguenti. Supponiamo che la nostra equazione irriducibile di grado primo p goda della proprietà che per due radici fisse, p. e. x_0, x_1, tutte le altre possano esprimersi razionalmente.

L'ordine m del gruppo transitivo dell'equazione sarà della forma

$$m = kp$$

e poichè la sola identità in G lascia ferme x_0, x_1, sarà m eguale al numero dei sistemi di posti che x_0, x_1 possono occupare per sostituzioni di G, cioè al massimo a $p(p-1)$, onde si rileva $k < p$. Ora G contiene certamente una sostituzione S a periodo p (ciclica sulle p radici) e quindi il gruppo ciclico

$$\Gamma_p = (1, S, S^2 \ldots S^{p-1}).$$

Se con U indichiamo una sostituzione di G fuori di Γ_p, le p^2 sostituzioni di G

$$S^\alpha U S^\beta \; \{ \alpha, \beta = 0, 1, 2 \ldots p-1$$

non potranno quindi essere tutte distinte, perchè $m < p^2$. Poniamo sia

$$S^\alpha U S^\beta = S^a U S^b,$$

con $\alpha \not\equiv a$. $\beta \not\equiv b \pmod p$. Ne deduciamo

$$U^{-1} S^{\alpha - a} U = S^{b-\beta}$$

e, determinando il numero r dalla congruenza

$$(\alpha - a) r \equiv 1 \pmod p,$$

segue

$$(U^{-1} S^{\alpha - a} U)^r = U^{-1} S U = S^{(b-\beta) r}.$$

Dunque U, trasformando S in una potenza di S, appartiene al gruppo metaciclico e quindi G coincide col gruppo metaciclico o con un suo sottogruppo d'ordine $p\delta$.

Possiamo dunque enunciare il teorema di Galois:

Affinchè un'equazione irriducibile di grado primo sia risolubile per radicali, è necessario e sufficiente che tutte le sue radici possano esprimersi razionalmente per due di esse.

Ora si osservi che se il campo di razionalità è reale: *l'equazione di* Galois *avrà in conseguenza una sola radice reale ovvero tutte le radici reali.* Come corollario, abbiamo dunque il teorema:

Se un'equazione irriducibile di grado primo, in un campo reale di razionalità, ha più di una radice reale, ma non tutte, essa è insolubile per radicali.

Dopo ciò è facilissimo formare nel campo assoluto di razionali delle equazioni irriducibili di grado primo p qualsiasi insolubili per radicali. Così p. e. l'equazione

$$f(x) = x^p + m\,q\,x^2 - q = 0\,,$$

essendo p, q numeri primi qualsiasi ed m un intero > 1, è irriducibile e non risolubile per radicali appena $p > 3$. Essa ha infatti *tre* radici reali, due negative ed una positiva [1]).

§. 88. — Il criterio per la risolubilità per radicali di un'equazione irriducibile di grado primo stabilito al §. precedente può trasformarsi in guisa da dargli anche un certo valore pratico sì da poter riconoscere, sopra una data equazione, se essa è o no risolubile. Per ciò costruiamo una funzione razionale y delle p radici

$$x_0\, x_1\, x_2 \ldots x_{p-1}$$

della proposta $f(x) = 0$, che rimanga numericamente invariata per tutte e sole le sostituzioni del gruppo metaciclico $G_{p(p-1)}$. Essa assumerà allora per tutte le $\pi(p)$ sostituzioni sulle radici

$$r = 1\,.\,2\,.\,3 \ldots (p-2)$$

valori numericamente distinti, che saranno le radici di una equazione razionalmente costruibile

$$(y - y_1)\;(y - y_2) \ldots (y - y_r) = 0\,.$$

Questa dicesi la *risolvente di* Lagrange della equazione proposta.

Ora, se la $f(x) = 0$ è risolubile per radicali, facilmente si vede che la risolvente di Lagrange avrà una radice razionale. E infatti, in tale ipotesi, il gruppo G della proposta sarà metaciclico quindi simile al gruppo costruito $G_{p(p-1)}$, o ad un suo sottogruppo d'ordine $p\delta$. Se T è una sostituzione sulle x che trasforma $G_{p(p-1)}$ (o un suo sottogruppo) nel gruppo di $f(x) = 0$, la radice y_T della risolvente di Lagrange, dedotta dalla prima y_1 colla sostituzione T, sarà allora razionalmente nota.

---

[1]) Si applichi la regola dei segni di Cartesio, osservando che

$$f(-\infty) < 0,\; f(-1) > 0,\; f(0) < 0,\; f(1) > 0\,.$$

Viceversa se una radice y_T della risolvente di LAGRANGE è razionale, il gruppo della proposta conterrà solo sostituzioni che la lasciano invariata e queste apparterranno quindi al gruppo metaciclico $T^{-1} G_{F(p-1)} T$, onde l'equazione sarà risolubile per radicali.

Abbiamo dunque il teorema:

La condizione necessaria e sufficiente affinchè un'equazione irriducibile di grado primo sia risolubile per radicali consiste in questo che la sua risolvente di LAGRANGE *abbia una radice razionale.*

Ai risultati esposti nei due §§. precedenti si lega una serie di ulteriori ricerche sulla effettiva formazione delle equazioni di grado primo metacicliche (a gruppo metaciclico) e sulla legge di costruzione delle formole che le risolvono per radicali. La soluzione completa di questo problema, formulato sotto altra forma da ABEL, è stata data da KRONECKER. Ma noi non possiamo qui addentrarci in tali studî ulteriori e solo ci contenteremo di esporre i risultati ottenuti da RUNGE [1]) per la costruzione delle equazioni metacicliche di 5.° grado della forma di BRING-JERRARD

$$x^5 + \alpha x + \beta = 0 , \tag{7}$$

alla quale, come è noto, può ridursi qualunque equazione di 5.° grado risolvendo soltanto un'equazione di 3.° grado [2]), e rimandiamo il lettore per maggiori notizie all'opera più volte citata di WEBER.

Si tratta di costruire in primo luogo per la equazione (7) la risolvente di LAGRANGE.

Indicando con

$$x_0, x_1, x_2, x_3, x_4$$

le radici della (7), queste potranno riguardarsi, finchè α, β restano indeterminati, come indipendenti. Le 20 sostituzioni del gruppo metaciclico sono generate dalle due fondamentali

$$S = (x_0 x_1 x_2 x_3 x_4) , \quad T = (x_1 x_2 x_4 x_3)$$

e le 10 del gruppo semimetaciclico da S e T^2. Una funzione razionale delle x che rimane invariata per S e T^2 e quindi per l'intero gruppo semimetaciclico è la seguente

$$y_1 = x_0 x_1 + x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_0 .$$

---

[1]) *Acta Mathematica*, Bd. 7.

[2]) V.i p. e. SERRET. — *Algèbre supérieure*, III.ème Édition §. 192.

Indicando con y_2 quella che se ne deduce per mezzo della T si ha

$$y_2 = x_0 x_2 + x_2 x_4 + x_4 x_1 + x_1 x_3 + x_3 x_0$$

e questa rimane ancora invariata pel gruppo ciclico generato da S, onde segue che posto

$$z_1 = y_1 - y_2$$

sarà z_1^2 una funzione invariabile per S e per T, quindi per l'intero gruppo metaciclico, mentre la z_1 resta invariata per la S e cangia segno per la T. Eseguendo sulle x le 60 sostituzioni del gruppo alterno, la z_1 acquista soltanto i 6 seguenti valori distinti

$$\begin{aligned}
z_1 &= (x_0 x_1 + x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_0) - \\
&\quad - (x_0 x_2 + x_2 x_4 + x_4 x_1 + x_1 x_3 + x_3 x_0) \\
z_2 &= (x_1 x_2 + x_2 x_4 + x_4 x_0 + x_0 x_3 + x_3 x_1) \\
&\quad - (x_1 x_4 + x_4 x_3 + x_3 x_2 + x_2 x_0 + x_0 x_1) \\
z_3 &= (x_2 x_4 + x_4 x_3 + x_3 x_1 + x_1 x_0 + x_0 x_2) \\
&\quad - (x_2 x_3 + x_3 x_0 + x_0 x_4 + x_4 x_1 + x_1 x_2) \\
z_4 &= (x_4 x_3 + x_3 x_0 + x_0 x_2 + x_2 x_1 + x_1 x_4) \\
&\quad - (x_4 x_0 + x_0 x_1 + x_1 x_3 + x_3 x_2 + x_2 x_4) \\
z_5 &= (x_3 x_0 + x_0 x_1 + x_1 x_4 + x_4 x_2 + x_2 x_3) \\
&\quad - (x_3 x_1 + x_1 x_2 + x_2 x_0 + x_0 x_4 + x_4 x_3) \\
z_6 &= (x_0 x_2 + x_2 x_3 + x_3 x_1 + x_1 x_4 + x_4 x_0) \\
&\quad - (x_0 x_3 + x_3 x_4 + x_4 x_2 + x_2 x_1 + x_1 x_0) ,
\end{aligned}$$

dei quali i primi quattro dopo z_1 sono dedotti da z_1 effettuandovi la sostituzione (0 1 2 4 3) e le sue potenze e l'ultimo z_6 colla sostituzione circolare (1 2 3) non equivalente, rispetto al gruppo semimetaciclico, alle dette potenze.

Questi sei valori sono dunque le radici di una risolvente di 6.° grado

$$z^6 + a_1 z^5 + a_2 z^4 + \ldots a_6 = 0 ,$$

i cui coefficienti sono razionalmente formati con $\sqrt{\Delta}$, essendo Δ il discriminante della proposta. Si osservi anzi di più che siccome per una sostituzione impari sulle x i 6 valori $z_1, z_2, z_3, z_4, z_5, z_6$ si cangiano in altro ordine, nei medesimi valori cangiati di segno, così ogni funzione omogenea simmetrica di $z_1, z_2, z_3, z_4, z_5, z_6$ resta invariata anche per le

sostituzioni impari sulle x se è di grado pari e cangia invece di segno se è di grado impari. Perciò a_2, a_4, a_6 sono funzioni intere simmetriche delle x mentre a_1, a_3, a_5 differiscono da una tale funzione simmetrica solo pel fattore $\sqrt{\Delta}$. Ora a_1, a_3, a_5 sono omogenee nelle x dei gradi 2, 6, 10 mentre $\sqrt{\Delta}$ è di grado 10; si ha dunque

$$a_1 = 0\,,\; a_3 = 0\,,\; a_5 = m\sqrt{\Delta}\,,$$

essendo m un coefficiente numerico e l'equazione di 6.° grado in z ha quindi la forma

$$z^6 + a_2 z^4 + a_4 z^2 + a_6 = m\sqrt{\Delta}\,.\,z \tag{8}$$

dove a_2, a_4, a_6 saranno funzioni razionali intere a coefficienti interi di α, β. Siccome poi α è della 4.ª, β della 5.ª dimensione nelle x mentre le dimensioni di a_2, a_4, a_6 sono rispettivamente 4, 8, 12, avremo necessariamente

$$a_2 = m_1\,\alpha,\;\; a_3 = m_2\,\alpha^2,\;\; a_6 = m_3\,\alpha^3$$

con m_1, m_2, m_3 interi. Per determinare i valori degli interi m_1, m_2, m_3, m basta dare ad α, β particolari valori e così facciamo $\alpha = -1$, $\beta = 0$ e si hanno per le 6 radici x i valori

$$0,\; i,\; i^2,\; i^3,\; i^4\,,$$

indi per le z_i quattro valori $= -2\,i$, uno $= 2 + 4\,i$ l'altro $= -2 + 4\,i$, mentre pel discriminante risulta $\Delta = -4^4$. Avremo quindi l'identità

$$z^6 - m_1 z^4 + m_2 z^2 - m_3 \pm 16\,i\,m z = (z + 2\,i)^4\,(z^2 - 8\,i z - 20) =$$
$$= z^6 + 20\,z^4 + 240\,z^2 - 320 + 512\,i\,z$$

onde:

$$(z^6 - m_1 z^4 + m_1 z^2 - m_3)^2 + 16^2\,m^2\,z^2 = (z^2 + 4)^4\,(z^4 + 24\,z^2 + 400)\,.$$

Ne deduciamo

$$m_1 = -20\,,\; m_2 = 240\,,\; m_3 = 320\,,\; m = \pm 2^5$$

e quindi la (8) liberata dal radicale $\sqrt{\Delta}$ diventa

$$(z^6 - 20\,\alpha\,z^4 + 240\,\alpha^2\,z^2 + 320\,\alpha^3)^2 = 4^5\,\Delta\,z^2\,.$$

Quanto al discriminante Δ esso è espresso per α, β colla formola

$$\Delta = 4^4 \alpha^5 + 5^5 \beta^4 .$$

La precedente equazione per z si può quindi anche scrivere nel modo seguente

$$(z^2 - 4\alpha)^4 (z^4 - 24\alpha z^2 + 400\alpha^2) = 4^5 . 5^5 \beta^4 z^2 .$$

Se poniamo

$$z^2 = 4y ,$$

potremo quindi scrivere l'equazione di 6.° grado in y sotto la forma

$$(y^3 - 5\alpha y^2 + 14\alpha^2 y + 5\alpha^3)^2 = \Delta y \tag{8}$$

o sotto la forma equivalente

$$(y - \alpha)^4 (y^2 - 6\alpha y + 25\alpha^2) = 5^5 \beta^4 y . \tag{9}$$

§. 90. — La funzione risolvente $y = \frac{z^2}{4}$ è certo invariabile per tutte le sostituzioni del gruppo metaciclico; ma, per potere riguardare la risolvente (8) o (9) come risolvente di Lagrange della proposta, bisogna che la y non rimanga numericamente invariata per alcuna altra sostituzione all'infuori del gruppo metaciclico, ossia che la risolvente (8) o (9) non abbia radici eguali. Ora perchè si presentino radici eguali occorre che insieme alla (8) sia soddisfatta l'equazione che si ottiene derivandola rispetto ad y, ovvero

$$2 (y^3 - 5\alpha y^2 + 15\alpha^2 y + 5\alpha^3) (3y^2 - 10\alpha y + 15\alpha^2) = \Delta$$

e sostituendo per Δ questo valore nella (8) stessa si trova subito

$$5 (y^3 - 5\alpha y^2 + 15\alpha^2 y + 5\alpha^3) (y - \alpha)^3 = 0$$

Se si annulla il primo fattore si ha per la (8) stessa $\Delta y = 0$, se si annulla il secondo risulta dalla (9) $\beta y = 0$. Se supponiamo la proposta irriducibile non potrà aversi nè $\Delta = 0$ nè $\beta = 0$; ma anche il caso $y = 0$ diventa allora impossibile perchè dovendosi annullare insieme il primo o secondo fattore dell'ultima espressione scritta, sarebbe anche $\alpha = 0$ e la (8) diventa $y^6 = \Delta y$ che non ammette $y = 0$ per radice multipla. Dunque:

Tutte le volte che la proposta (7)

$$x^5 + \alpha x + \beta = 0$$

è irriducibile, la (8) *o* (9) *è la sua risolvente di* LAGRANGE *e però la proposta sarà risolubile per radicali allora e allora soltanto che la* (8) *o* (9) *abbia una radice razionale.*

Si osservi poi che se la proposta è riducibile essa è certamente risolubile per radicali per cui siamo ora completamente in grado di giudicare se una equazione di 5.° grado della forma di BRING: $x^5 + \alpha x + \beta = 0$ è o no solubile per radicali.

Se supponiamo in particolare che α, β siano numeri interi, la risolvente stessa (8) o (9) ha coefficienti interi e il primo eguale all'unità, onde le sue eventuali radici razionali saranno interi divisori del termine costante $25\ \alpha^6$. Facciamo p. e.

$$\alpha = 5 \qquad \beta = 5\,m\ ,$$

essendo m un intero non divisibile per 5; l'equazione corrispondente

$$x^5 + 5\,x + 5\,m = 0$$

è irriducibile. Una eventuale radice intera della (9) dovrebbe essere un divisore di 5^8 ciò che subito si vede non aver luogo. Dunque:

Ogni equazione di 5.° grado della forma

$$x^5 + 5\,x + 5\,m = 0\,;$$

con m intero non divisibile per 5, è insolubile per radicali.

Al contrario se facciamo $\alpha = 0$ e diamo a β un valore intero qualunque che non sia una 5.ª potenza esatta, l'equazione

$$x^5 + \beta = 0$$

è irriducibile (§. 80) e solubile per radicali.

Per costruire tutte le equazioni

$$x^5 + \alpha\,x + \beta = 0$$

risolubili, pongasi

$$y = \alpha\,\lambda\ ,\ \beta = \alpha\,\mu$$

e si sostituiscano questi valori nella (9); si otterrà

$$\begin{cases} \alpha = \dfrac{5^5\,.\,\mu^4\,\lambda}{(\lambda-1)^4\,(\lambda^2-6\,\lambda+25)} \\[2ex] \beta = \dfrac{5^5\,\mu^5\,\lambda}{(\lambda-1)^4\,(\lambda^2-6\,\lambda+25)} \end{cases}$$

Dando a λ, μ valori razionali in qualsiasi campo di razionalità si avrà un'equazione (7) risolubile, risulti questa irriducibile o riducibile.

Capitolo VII [1]).

Le equazioni di Gauss per la divisione del circolo in parti eguali. — I periodi di Gauss e le successive risolventi. — Poligoni regolari costruibili elementarmente. — La risolvente di 2.° grado e il teorema di reciprocità pei residui quadratici. — I numeri complessi $\psi_n(\alpha)$.

§. 91. — Nel presente capitolo ci proponiamo di applicare le teorie generali fin qui svolte al classico esempio delle equazioni per la divisione del circolo in m parti eguali per far conoscere, almeno nei suoi tratti essenziali, la teoria di Gauss che ha preceduto e preparato le ricerche di Abel e di Galois, e dove appunto i teoremi generali trovano la più semplice ed elegante conferma.

Il problema di *inscrivere nel circolo il poligono regolare di m lati* corrisponde algebricamente a quello della risoluzione dell'equazione binomia

$$x^m = 1. \tag{1}$$

Nota infatti la particolare radice

$$\varepsilon = \cos\frac{2\pi}{m} + i \operatorname{sen}\frac{2\pi}{m}$$

di questa equazione, conosceremo le linee trigometriche dell'arco di cerchio (di raggio = 1) che sottende il lato del poligono cercato.

Osserviamo subito che potremmo limitare le nostre ricerche al caso in cui m sia la potenza di un numero primo p. E invero, se risolviamo m nei suoi fattori primi

$$m = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n} ,$$

essendo $p_1, p_2 \dots p_n$ i divisori primi diversi di m, i numeri

$$\frac{m}{p_1^{r_1}}, \frac{m}{p_2^{r_2}} \dots \frac{m}{p_n^{r_n}}$$

non hanno alcun divisore comune ed è quindi risolubile in numeri interi α l'equazione

$$\frac{m}{p_1^{r_1}}\alpha_1 + \frac{m}{p_2^{r_2}}\alpha_2 + \dots + \frac{m}{p_n^{r_n}}\alpha_n = 1$$

---

[1]) Le teorie del presente Capitolo sono ampiamente svolte nel libro di Bachmann, *Die Lehre von der Kreistheilung,* (Leipzig-Teubner 1872), al quale ci uniformiamo in questo rapido sunto.

e si ha perciò

$$\frac{2\pi}{m} = \alpha_1 \frac{2\pi}{p_1^{r_1}} + \alpha_2 \frac{2\pi}{p_2^{r_2}} + \ldots + \alpha_n \frac{2\pi}{p_n^{r_n}} .$$

Potremo dunque comporre l'arco $\frac{2\pi}{m}$ appena noti gli archi

$$\frac{2\pi}{p_1^{r_1}}, \frac{2\pi}{p_2^{r_2}} \ldots \frac{2\pi}{p_n^{r_n}},$$

la cui ricerca corrisponde appunto al caso in cui m sia la potenza di un numero primo.

In altre parole possiamo dire che ogni radice m^{ma} dell'unità è data da

$$\varepsilon = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_n ,$$

essendo $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n$ rispettivamente radici dell'unità d'ordini $p_1^{r_1}, p_2^{r_2}, \ldots p_n^{r_n}$. Si otterranno in particolare tutte le radici primitive m^{me} facendo percorrere rispettivamente ad $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_n$ le corrispondenti radici primitive.

Ma dapprima esporremo alcune considerazioni sul caso generale in cui m sia un numero composto qualunque, specialmente allo scopo di scindere la funzione

$$x^m - 1$$

nei suoi fattori irriducibili e di determinare il gruppo di Galois per ogni equazione corrispondente. Per questo ricordiamo che tutte le radici della (1) sono date da

$$e^{\frac{2\pi i r}{m}} \quad r = 0, 1, 2 \ldots m-1$$

e che fra queste sono radici primitive quelle in cui r è primo con m; il numero delle radici primitive è $\varphi(m)$. Ogni altra radice non primitiva, ove r abbia con m un massimo comun divisore $\delta > 1$, è radice dell'altra equazione binomia di grado inferiore m divisore di m

$$x^{\frac{m}{\delta}} = 1 .$$

Coi noti processi razionali possiamo liberare la equazione (1) da tutte le radici che essa ha a comune con queste equazioni di grado inferiore

e formare così un'equazione a *coefficienti razionali* di grado $\nu = \varphi(m)$, che indicheremo con

$$X_m(x) = x^\nu + a_1 x^{\nu-1} + a_2 x^{\nu-2} + \ldots + a_\nu = 0,$$

le cui radici saranno tutte e sole le $\varphi(m)$ radici primitive m^{me} dell'unità.

§. 92. — Per procedere alla costruzione effettiva di questi polinomii X_m cominciamo dal caso particolare in cui m sia la potenza di un numero primo $m = p^r$. Tutte le radici *non primitive* di $x^{p^r} = 1$ soddisfano all'altra equazione $x^{p^{r-1}} = 1$ e si ha per ciò immediatamente

$$(2)\quad X_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{p^{r-1}(p-1)} + x^{p^{r-1}(p-2)} + \ldots + x^{p^{r-1}} + 1 .$$

Supponendo ora di conoscere $X_m(x)$ mostriamo come si formerà l'altro polinomio

$$X_{mp^r}(x),$$

dove p è un numero primo che non divide m; avremo allora evidentemente un modo di costruire uno qualunque dei nostri polinomi. A tale scopo dimostriamo la formola

$$(3)\qquad X_{mp^r}(x) = \frac{X_m(x^{p^r})}{X_m(x^{p^{r-1}})},$$

ciò che facciamo osservando le proprietà seguenti:

1.ª I fattori lineari del numeratore $X_m(x^{p^r})$ come del denominatore $X_m(x^{p^{r-1}})$ sono tutti semplici; infatti una radice x multipla di

$$X_m(x^{p^r}) = 0$$

dovrebbe soddisfare l'equazione derivata

$$x^{p^{r-1}} X'_m(x^{p^r}) = 0,$$

ciò che è assurdo poichè $X_m(0) \neq 0$ e X_m, X'_m non hanno fattori comuni.

2.ª Tutti i valori di x che annullano il denominatore annullano anche il numeratore; poichè da $x^{p^{r-1}} = \varepsilon$, essendo ε una radice primitiva m^{ma} dell'unità, segue $x^{p^r} = \varepsilon^p$ che è ancora una tale radice primitiva, p non dividendo m.

3.ª Tutti i valori di x che annullano il numeratore, senza annullare il denominatore, annullano anche $X_{mp^r}(x)$; e viceversa ogni radice di $X_{mp^r}(x)$ è radice del numeratore senza esserlo del denominatore.

E infatti se x^{p^r} è radice primitiva m^{ma} e non lo è $x^{p^{r-1}}$ si ha $x^{mp^r} = 1$ e quindi $x = e^{\frac{2k\pi i}{mp^r}}$ dove k sarà primo con m, altrimenti x^{p^r} non sarebbe radice primitiva m^{ma}, e non divisibile per p altrimenti $x^{p^{r-1}}$ sarebbe radice primitiva m^{ma}, onde x è radice primitiva d'ordine mp^r cioè annulla $X_{mp^r}(x)$ c. d. d. L'inversa si vede egualmente.

Dimostrata così la formola (3), applicando questa e la (2) vediamo subito che se $m = p_1^{r_1} p_2^{r_2}$ contiene due soli fattori primi diversi p_1, p_2, avremo

$$X_m(x) = \frac{(x^m - 1)\ (x^{\frac{m}{p_1 p_2}} - 1)}{(x^{\frac{m}{p_1}} - 1)\ (x^{\frac{m}{p_2}} - 1)} .$$

Nel caso generale indichiamo con μ_1 tutti i divisori di m (m compreso) della forma

$$m\,,\ \frac{m}{p_i p_k}\,,\ \frac{m}{p_i p_k p_l p_m}\,, \ldots$$

che si ottengono dividendo m per un numero pari di suoi divisori primi diversi e similmente con μ_2 tutti i divisori della forma

$$\frac{m}{p_i}\,,\ \frac{m}{p_i p_k p_l}\,, \ldots$$

che si ottengono dividendo m per un numero dispari di tali fattori; avremo la formola

$$X_m(x) = \frac{\prod\limits_{\mu_1}(x^{\mu_1} - 1)}{\prod\limits_{\mu_2}(x^{\mu_2} - 1)}\,, \tag{4}$$

i prodotti al numeratore e denominatore essendo rispettivamente estesi ai divisori μ_1 e μ_2.

E infatti la (4) è vera se m contiene uno o due soli fattori primi diversi e dalla (3) risulta che se è vera per m lo è anche per mp^r, essendo p un numero primo che non divide m.

La (4) ci dimostra che il polinomio $X_m(x)$ ha per primo coefficiente l'unità e gli altri sono tutti numeri interi. Si osservi poi che il numero

intero $X_m(1)$ è eguale al numero primo p se m è la potenza di un numero primo p, come si vede dalla (2). Se invece m contiene due o più fattori primi diversi, segue facilmente dalla (3): $X_m(1) = 1$. Abbiamo dunque il risultato:

Il numero $X_m(1)$ *è eguale al numero primo* p *o all'unità, secondo che* m *contiene un solo divisore primo o ne contiene diversi.*

§. 93. — Dimostriamo ora col metodo di KRONECKER l'importante teorema:

Il polinomio $X_m(x)$ *è irriducibile nel campo assoluto di razionalità.*

Supponiamo al contrario che X_m si spezzi nei due fattori razionali

$$X_m(x) = \varphi(x) \cdot \psi(x),$$

dove, pei teoremi di GAUSS dimostrati al §. 59, potremo supporre che $\varphi(x)$, $\psi(x)$ abbiano il primo coefficiente $= 1$ e gli altri numeri interi. Facendo nella precedente $x = 1$, avremo

$$\varphi(1) \cdot \psi(1) = X_m(1)$$

e poichè $X_m(1)$ o è eguale a 1 o ad un numero primo p, uno dei due fattori $\varphi(1)$, $\psi(1)$ sarà necessariamente $= \pm 1$, sia p. e.

$$\varphi(1) = \pm 1. \tag{5}$$

Ora le radici di $\varphi(x) = 0$ sono certamente fra le radici primitive m^{me} dell'unità e poichè, indicando con ε una *qualunque* radice primitiva, tutte le altre sono potenze di ε, sarà necessariamente

$$\varphi(\varepsilon)\ \varphi(\varepsilon^2)\ \varphi(\varepsilon^3) \ldots \varphi(\varepsilon^{m-1}) = 0,$$

ossia

$$\Phi(x) = \varphi(x) \cdot \varphi(x^2)\, \varphi(x^3) \ldots \varphi(x^{m-1}) \tag{6}$$

si annulla per tutte le radici di $X_m = 0$ ed è perciò $\Phi(x)$ divisibile per $X_m(x)$, poniamo

$$\Phi(x) = X_m(x)\, \Theta(x). \tag{7}$$

Poichè $\Phi(x)$ ha, come $X_m(x)$, per primo coefficiente 1 e gli altri interi, sarà $\Theta(x)$ un polinomio della medesima natura. Ora dalla (5), (6) segue $\Phi(1) = \pm 1$ e facendo $x = 1$ nella (7) otteniamo

$$\pm 1 = X_m(1)\, \Theta(1),$$

ove $\Theta(1)$ sarà un intero. Se m è la potenza di un numero primo p, la precedente è assurda perchè $X_n(1) = p$; dunque il polinomio $X_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}$ è irriducibile.

Per dimostrare ora la proprietà in generale basterà provare che se m si scinde nel prodotto $m = r.s$ di due fattori r, s, che siano primi fra loro, il polinomio $X_m(x)$ sarà irriducibile, supposto che tali siano i due $X_r(x)$, $X_s(x)$. Sia al contrario $\varphi(x)$ un fattore razionale di $X_m(x)$, che potremo supporre al solito col primo coefficiente $= 1$ e gli altri numeri interi. Ogni radice ρ di $\varphi(x) = 0$ è una radice di $X_m = 0$ e come tale (r, s essendo primi fra loro) decomponibile nel prodotto

$$\rho = \alpha\beta$$

di una radice α di $X_r(x) = 0$ per una radice β di $X_s(x) = 0$. Le potenze r^{me}

$$\rho^r = \beta^r$$

delle radici di $\varphi(x) = 0$ sono quindi radici di $X_s(x) = 0$. Costruendo dunqne la trasformata di Tschirnhaus $\Phi(x) = 0$ che ha per radici le r^{me} potenze delle radici di $\varphi(x) = 0$, avremo un polinomio $\Phi(x)$ a coefficienti interi, le cui radici sono radici di $X_s(x) = 0$ e però, essendo $X_s(x)$ irriducibile, le esauriscono tutte. Dunque le ρ^r, percorrendo ρ tutte le radici di $\varphi(x) = 0$, e per ciò anche le β, esauriscono tutte le radici di $X_s(x)$ e, per la stessa ragione, le α esauriscono le radici di $X_r(x)$. Ne segue che ogni radice di $X_m(x)$ appartiene anche a $\varphi(x)$ contro l'ipotesi che $\varphi(x)$ fosse soltanto un fattore di X_m.

§. 94. — L'equazione alle radici primitive m^{me}

$$X_m(x) = 0 \tag{8}$$

è, come si è visto, irriducibile nel campo assoluto di razionalità. Dopo ciò basterà che dimostriamo il carattere Abeliano di questa equazione per determinarne il gruppo di Galois. Indichiamo con

$$r_1, r_2, r_3 \ldots r_\nu \quad (\nu = \varphi(m)) \tag{9}$$

un sistema completo di resti (mod m), esclusi quelli non primi con m; di

questi ν numeri (9) uno sarà $\equiv 1 \pmod{m}$, poniamo sia $r_1 \equiv 1 \pmod{m}$. Se ε è una qualunque radice primitiva m^{ma} p. e.

$$\varepsilon = e^{\frac{2\pi i}{m}},$$

le ν radici della (8) sono

$$x_{r_1} = \varepsilon^{r_1}, \; x_{r_2} = \varepsilon^{r_2}, \ldots x_{r_\nu} = \varepsilon^{r_\nu},$$

cioè sono tutte funzioni razionali di una qualunque di esse e si ha inoltre la permutabilità delle corrispondenti operazioni

$$\Theta_i(\varepsilon) = \varepsilon^{r_i},$$

giacchè

$$\Theta_i(\Theta_k(\varepsilon)) = \Theta_k(\Theta_i(\varepsilon)) = \varepsilon^{r_i r_k}.$$

Dunque (§. 73) l'equazione (8) è Abeliana e il suo gruppo G consta di ν sostituzioni

$$g_1, g_2, g_3 \ldots g_\nu$$

due a due permutabili. Se indichiamo precisamente con g_i la sostituzione che porta ε in ε^{r_i}, applicando alla relazione

$$x_{r_k} = \varepsilon^{r_k}$$

la g_i, vediamo che g_i trasporta ogni altra radice ε^{r_k} in $\varepsilon^{r_i r_k}$; dunque la g_i moltiplica i ν numeri (9) tutti per r_i, cangiandoli nei numeri

$$r_i r_1, \; r_i r_2, \; r_i r_3 \ldots r_i r_\nu,$$

che rispetto al modulo m sono i numeri (9) stessi in altro ordine. Così adunque: *Il gruppo di* Galois *per l'equazione* (8) *sulle radici* m^{me} *dell'unità, denotando con*

$$x_{r_1}, x_{r_2} \ldots x_{r_\nu}$$

le ν *radici, è analiticamente rappresentato dalle sostituzioni lineari*

$$\mu' \equiv a\mu \pmod{m}$$

sugli indici μ *delle radici, il moltiplicatore* a *percorrendo i* $\nu = \varphi(m)$ *numeri primi con* m.

Applicando a questo gruppo Abeliano i risultati generali dei §§. 30-34 relativi alla decomposizione del gruppo in gruppi parziali e alla ricerca di una base del gruppo, saremmo condotti a quel capitolo della teoria

dei numeri che tratta della formazione di un sistema d'indici pei numeri composti [1]).

In particolare si vede che il nostro gruppo è ciclico soltanto quando m è la potenza di un numero primo dispari o il doppio di una tale potenza, esclusi i casi particolari $m = 2$, $m = 4$.

Osserviamo ora che posto

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} ,$$

si ha

$$\nu = \varphi(m) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_n^{\alpha_n - 1} (p_1 - 1)(p_2 - 1) \dots (p_n - 1) ,$$

sicchè per risolvere la proposta, oltre le estrazioni di radicali di indici corrispondenti ai divisori primi dei numeri

$$p_1 - 1 , p_2 - 1 \dots p_n - 1 ,$$

dobbiamo ancora estrarre $\alpha_1 - 1$ radicali d'indice $= p_1$, $\alpha_2 - 1$ radicali d'indice $= p_2$ ecc.

Perchè il corrispondente problema geometrico sia risolubile colla riga e col compasso è necessario e sufficiente che gli indici di questi radicali siano tutti $= 2$ [2]).

Abbiamo dunque il teorema di Gauss:

Perchè il poligono regolare di m lati sia costruibile elementarmente (colla riga e col compasso) è necessario e sufficiente che i fattori primi dispari di m entrino in m alla prima potenza soltanto e siano tutti della forma $p = 2^n + 1$.

I casi $p = 3$, $p = 5$ per numeri primi e i conseguenti

$$m = 2^n , 2^n . 3 , 2^n . 5 , 2^n . 3 . 5$$

per numeri composti, erano già noti nell'antichità. La teoria di Gauss ha fatto conoscere i nuovi casi

$$p = 17, 257, 65537 \dots$$

e i composti da questi.

---

[1]) Cf. Dirichlet-Dedekind. — *Zahlentheorie*, Suppl, V.

[2]) Un problema geometrico determinato risolubile colla riga e col compasso deve condurre ad un'equazione che si risolva estraendo soltanto radici quadrate. Bisogna per ciò (§. 80) che l'ordine del gruppo sia una potenza del 2 e tale deve essere anche il grado della equazione, supposta irriducibile.

Rispetto ai numeri primi della forma

$$p = 2^n + 1$$

è stato osservato che l'esponente n stesso deve essere una potenza del 2, perchè se fosse $n = 2^\mu (2r+1)$, essendo già $x^{2r+1}+1$ algebricamente divisibile per $x+1$, il numero $2^{2^\mu(2r+1)}+1$ avrebbe il divisore $2^{2^\mu}+1$. Però l'ipotesi di Fermat che tutti i numeri della forma $2^{2^\mu}+1$ fossero primi è stata riconosciuta erronea. I casi noti di numeri composti di questa forma sono i quattro seguenti

$$2^{2^5}+1 \text{ (Eulero)}, \quad 2^{2^6}+1 \text{ (Landey)}$$

$$2^{2^{12}}+1 \text{ (Pervouchine)}, \quad 2^{2^{23}}+1 \text{ (Pervouchine-Lucas)}.$$

Del resto, fino ad oggi, non è nemmen noto se nella serie $2^{2^\mu}+1$ vi siano o no infiniti numeri primi.

§. 95. — Nelle ricerche seguenti ci restringeremo al caso fondamentale della equazione

$$X_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0, \tag{10}$$

dove p è un numero primo. Ci proponiamo in questo caso di costruire e studiare le diverse risolventi, la cui esistenza ci è rivelata dai teoremi generali.

Se indichiamo con ε una qualunque radice della (10) e con g una radice primitiva (mod p), il gruppo della (10), per quanto si è visto sopra, è il gruppo ciclico Γ_{p-1} generato dalle potenze della sostituzione ciclica

$$S = (\varepsilon, \varepsilon^g, \varepsilon^{g^2}, \ldots \varepsilon^{g^{p-2}}).$$

Per costruire una risolvente della (10) dobbiamo prendere un sottogruppo Γ di G_{p-1} ed assumere una funzione razionale delle radici della (10) numericamente invariabile per tutte le sostituzioni di Γ. Se indichiamo con S^e la minima potenza di S che figura in Γ (cioè con e il periodo relativo di S rispetto a Γ) tutte le altre sostituzioni di Γ saranno potenze di S^e ed e dovrà essere un divisore di $p-1$; poniamo

$$p - 1 = ef$$

ed avremo:

$$S^e = (\varepsilon, \varepsilon^{g^e}, \varepsilon^{g^{2e}} \ldots \varepsilon^{g^{(f-1)e}}) \,.\, (\varepsilon^g, \varepsilon^{g^e+1}, \varepsilon^{g^{2e}+1} \ldots \varepsilon^{g^{(f-1)e}+1}) \ldots (\varepsilon^{g^{e-1}}, \varepsilon^{g^{2e-1}} \ldots \varepsilon^{g^{ef-1}}) \,.$$

Ora una funzione invariabile per la S^e, quindi per tutto Γ, è data semplicemente da

$$\eta_0 = \varepsilon + \varepsilon^{g^e} + \varepsilon^{g^{2e}} + \ldots + \varepsilon^{g^{(f-1)e}}$$

e i valori che essa assume per le sostituzioni di G_{p-1}, e che proveremo ora essere numericamente diversi, sono gli e seguenti

$$(11) \qquad \begin{cases} \eta_0 = \varepsilon + \varepsilon^{g^e} + \varepsilon^{g^{2e}} + \ldots + \varepsilon^{g^{(f-1)e}} \\ \eta_1 = \varepsilon^g + \varepsilon^{g^e+1} + \varepsilon^{g^{2e}+1} + \ldots + \varepsilon^{g^{(f-1)e}+1} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \eta_{e-1} = \varepsilon^{g^{e-1}} + \varepsilon^{g^{2e-1}} + \varepsilon^{g^{3e-1}} + \ldots + \varepsilon^{g^{fe-1}} \,. \end{cases}$$

Queste espressioni diconsi i *periodi di* Gauss e per provare che essi sono numericamente distinti basta appoggiarsi sulla dimostrata irriducibilità della (10). Se si avesse infatti

$$\eta_h = \eta_k \,,$$

cioè

$$\varepsilon^{g^h} + \varepsilon^{g^{h+e}} + \ldots + \varepsilon^{g^{h+(f-1)e}} = \varepsilon^{g^k} + \varepsilon^{g^{k+e}} + \ldots + \varepsilon^{g^{k+(f-1)e}} \,,$$

riducendo ciascun esponente g^{u} al minimo resto positivo (mod p) e dividendo l'equazione per ε, si avrebbe un'equazione, di grado $p-2$ al massimo, a coefficienti interi, cui soddisferebbe ε, cioè la (10) sarebbe riducibile.

Gli e periodi η di Gauss sono radici di una risolvente di grado e, che indicheremo con

$$(12) \qquad F_e(\eta) = (\eta - \eta_0)(\eta - \eta_1) \ldots (\eta - \eta_{e-1}) \,.$$

Questa risolvente ha il primo coefficiente $= 1$ e gli altri, in ordine ai teoremi generali, sono numeri razionali. Ma di più possiamo dimostrare che questi coefficienti sono interi.

Ciò risulta come caso particolare dal teorema generale:

Qualunque funzione razionale intera a coefficienti interi delle radici

della (10), *numericamente invariabile per le sostituzioni del gruppo* G_{p-1}, *è eguale ad un numero intero* [1]).

E invero una tale funzione

$$\Phi(\varepsilon, \varepsilon^g, \varepsilon^{g^2}, \ldots \varepsilon^{g^{p-2}})$$

si potrà in primo luogo porre sotto la forma

$$\Phi = a_0 + a_1 \varepsilon + a_2 \varepsilon^g + a_3 \varepsilon^{g^2} + \ldots + a_{p-1} \varepsilon_g^{p-2},$$

le a essendo numeri interi, indi, osservando che si ha

$$\varepsilon + \varepsilon^g + \varepsilon^{g^2} + \ldots + \varepsilon^{g^{p-2}} = -1,$$

sotto l'altra

$$\Phi = \alpha_0 \varepsilon + \alpha_1 \varepsilon^g + \alpha_2 \varepsilon^{g^2} + \ldots + \alpha_{p-2} \varepsilon^{g^{p-2}}$$

colle α nuovamente intere. Questa si dirà la *forma normale* della Φ. Tale forma normale è unica perchè, supposto

$$\sum_{r=0}^{r=p-2} \alpha_r \varepsilon^{g^r} = \sum_{r=0}^{r=p-2} \beta_r \varepsilon^{g^r},$$

se le β non coincidessero colle corrispondenti α se ne trarrebbe, come sopra, la conseguenza che la (10) sarebbe riducibile. Ora se la Φ è numericamente invariabile per la S, avremo

$$\alpha_0 \varepsilon + \alpha_1 \varepsilon^g + \alpha^2 \varepsilon^{g^2} + \ldots + \alpha_{p-2} \varepsilon^{g^{p-2}} = \alpha_0 \varepsilon^g + \alpha_1 \varepsilon^{g^2} + \alpha_2 \varepsilon^{g^3} + \ldots + \alpha_{p-2} \varepsilon,$$

indi per l'osservazione superiore

$$\alpha_0 = \alpha_1 = \alpha_2 = \ldots = \alpha_{p-2}$$

e però

$$\Phi = \alpha_0 (\varepsilon + \varepsilon^g + \ldots + \varepsilon^{g^{p-2}}) = -\alpha_0,$$

ciò che dimostra il teorema.

---

[1]) Il teorema del testo non è alla sua volta che un caso particolare dell'altro, appartenente alla teoria dei numeri interi algebrici:

Se un'equazione $f(x) = 0$ *ha per primo coefficiente* 1 *e gli altri interi, qualunque funzione razionale intera delle sue radici, che sia razionalmente nota, è eguale ad un numero intero.* (V^i. p. e. DEDEKIND Suppl. X alla *Zahlentheorie* di Dirichlet).

§. 96. — La sostituzione

$$S = (\varepsilon, \varepsilon^g, \varepsilon^{g^2} \ldots \varepsilon^{g^{p-2}})$$

produce sui periodi η di GAUSS la sostituzione ciclica

$$U = (\eta_0\, \eta_1\, \eta_2 \ldots \eta_{e-1}).$$

Il gruppo della risolvente è quindi (§. 70) il gruppo ciclico

$$G_e = (1, U, U^2, \ldots U^{e-1})$$

e la $F_e(\eta) = 0$ è alla sua volta un'equazione Abeliana irriducibile a gruppo ciclico.

Per risolverla occorre aggiungere al campo assoluto di razionalità la radice primitiva dell'unità d'ordine e

$$\rho = \cos\frac{2\pi}{e} + i \operatorname{sen}\frac{2\pi}{e}$$

ed estrarre indi un radicale d'indice e (§. 74).

Risoluta la $F_e(\eta) = 0$, il gruppo G_{p-1} della proposta si riduce al sottogruppo Γ_f formato dalle potenze di S^e. Ogni funzione razionale delle radici della proposta invariabile per S^e è quindi razionalmente esprimibile per i periodi $\eta_0, \eta_1 \ldots \eta_{e-1}$ di GAUSS. Ma nel caso nostro possiamo dare al risultato una forma più determinata, dimostrando il teorema:

Ogni funzione razionale intera a coefficienti interi di $\varepsilon, \varepsilon^g, \varepsilon^{g^2} \ldots \varepsilon^{g^{p-2}}$, *numericamente invariabile per la* S^e, *si può esprimere per una funzione lineare intera ed omogenea a coefficienti interi dei periodi* $\eta_0, \eta_1 \ldots \eta_{e-1}$.

Poniamo infatti una tale funzione Φ sotto la forma normale

$$\Phi = \sum_{r=0}^{r=p-2} \alpha_r\, \varepsilon^{g^r},$$

le α essendo numeri interi. Avremo per ipotesi

$$\sum_r \alpha_r\, \varepsilon^{g^r} = \sum_r \alpha_r\, \varepsilon^{g^{e+r}},$$

onde (§. 95)

$$\alpha_0 = \alpha_e = \alpha_{2e} = \ldots = \alpha_{(f-1)e}$$

$$\alpha_1 = \alpha_{e+1} = \alpha_{2e+1} = \ldots = \alpha_{(f-1)e+1}$$

$$\cdots\cdots\cdots\cdots$$

e però

$$\Phi = \alpha_0 \eta_0 + \alpha_1 \eta_1 + \ldots + \alpha_{e-1} \eta_{e-1} ,$$

ciò che dimostra il teorema.

In particolare si osservi che il prodotto di due o più periodi η sarà esprimibile sotto la forma indicata.

L'equazione $F_e(\eta) = 0$ essendo Abeliana, basterà conoscere una sua radice a per averle tutte. Ora, supposta nota una tale radice a, si può domandare a quale dei periodi η è eguale; siccome per altro con ε abbiamo indicato una qualunque radice della (10), potremo evidentemente supporre $\eta_0 = a$. Si troveranno allora le altre radici osservando che, pel teorema superiore, si ha

$$\begin{cases} \eta_0^2 = a_0 \eta_0 + a_1 \eta_1 + \ldots + a_{e-1} \eta_{e-1} \\ \eta_0^3 = b_0 \eta_0 + b_1 \eta_1 + \ldots + b_{e-1} \eta_{e-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \eta_0^{e-1} = g_0 \eta_0 + g_1 \eta_1 + \ldots + g_{e-1} \eta_{e-1} , \end{cases}$$

le $a, b, \ldots g$ essendo interi. Aggiungendo a queste equazioni lineari l'altra

$$-1 = \eta_0 + \eta_1 + \eta_2 \ldots + \eta_{e-1}$$

si potranno risolvere queste $e-1$ equazioni lineari rispetto ad $\eta_1, \eta_2 \ldots \eta_{e-1}$, giacchè non possono essere linearmente dipendenti; altrimenti ne risulterebbe per η_0 un'equazione a coefficienti interi di grado $e-1$, mentre la $F_e(\eta) = 0$ è irriducibile. Così si esprimeranno $\eta_1, \eta_2 \ldots \eta_{e-1}$ razionalmente per η_0.

§. 97. — Fra le funzioni cui è applicabile il teorema del §. precedente trovansi evidentemente le seguenti

$$(x - \varepsilon^{g^h})(x - \varepsilon^{g^{h+e}})(x - \varepsilon^{g^{h+2e}}) \ldots (x - \varepsilon^{g^{h+(f-1)e}}) ,$$
$$(h = 0, 1, 2 \ldots, e-1) ,$$

la x essendo un'indeterminata. Per la risoluzione di $F_e(\eta) = 0$ la proposta si scinde quindi in e fattori razionali di grado f, come risulta anche dalla teoria generale. Dopo di ciò basta quindi risolvere l'equazione di grado f:

$$(13) \qquad (x - \varepsilon)(x - \varepsilon^{g^e}) \ldots (x - \varepsilon^{g^{(f-1)e}}) = 0 ,$$

i cui coefficienti sono funzioni lineari intere a coefficienti interi dei periodi η.

Nel campo ampliato di razionalità la (13) ha per gruppo il gruppo ciclico generato dalla sostituzione

$$V = (\varepsilon, \varepsilon^{g^e}, \varepsilon^{g^{2e}} \ldots \varepsilon^{g^{(f-1)e}})$$

a periodo f ed è quindi un'equazione Abeliana irriducibile di grado f.

Sopra di esse potremo quindi procedere come sulla proposta e se f è scindibile in due fattori

$$f = e' f',$$

se ne potrà costruire una risolvente di grado e' le cui radici saranno

$$\begin{cases} \eta'_0 = \varepsilon + \varepsilon^{g^{e'e}} + \varepsilon^{g^{2e'e}} + \ldots + \varepsilon^{g^{(f'-1)e'e}} \\ \eta'_1 = \varepsilon^{g^e} + \varepsilon^{g^{(e'+1)e}} + \varepsilon^{g^{(2e'+1)e}} + \ldots + \varepsilon^{g^{[(f'-1)e'+1]e}} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \eta'_{e'-1} = \varepsilon^{g^{(e'-1)e}} + \varepsilon^{g^{(2e'-1)e}} + \ldots + \varepsilon^{g^{(f'e'-1)e}}. \end{cases}$$

I coefficienti di questa risolvente

$$\Phi_{e'}(\eta') = (\eta' - \eta'_0)(\eta' - \eta'_1) \ldots (\eta' - \eta'_{e'-1}) = 0$$

saranno funzioni lineari intere a coefficienti interi di $\eta_0, \eta_1 \ldots \eta_{e-1}$ e la $\Phi_{e'}(\eta') = 0$ sarà un'equazione Abeliana irriducibile, che si risolve estraendo un radicale d'indice e'. Dopo ciò sarà razionalmente noto il fattore

$$(x - \varepsilon)(x - \varepsilon^{g^{e'e}}) \ldots (x - \varepsilon^{g^{(f'-1)e'e}})$$

di grado f' della proposta, che eguagliato a zero darà un'equazione Abeliana irriducibile nel nuovo campo. Su questa potremo procedere nella medesima guisa, scindendo f' in due fattori: $f' = e'' f''$ e così via.

Se per i fattori $e, e', e'' \ldots$ prendiamo i successivi fattori primi di $p - 1$, essendo

$$p - 1 = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

ritroviamo nuovamente il teorema al §. 78.

L'ordine secondo cui assumiamo i fattori primi di $p - 1$ nella serie e, e', e'' è naturalmente in nostro arbitrio. Sarà però utile ritenere come

ultimo fattore il 2 in guisa che gli ultimi periodi da determinarsi siano i binarii

$$\varepsilon+\varepsilon^{g^{\frac{p-1}{2}}}, \quad \varepsilon^{g}+\varepsilon^{g^{\frac{p-1}{2}+1}}, \quad \varepsilon^{g^2}+\varepsilon^{g^{\frac{p-1}{2}+2}} \ldots$$

cioè

$$\varepsilon+\varepsilon^{-1}, \quad \varepsilon^{g}+\varepsilon^{-g}, \quad \varepsilon^{g^2}+\varepsilon^{-g^2} \ldots$$

Questi ultimi periodi saranno quindi reali e reali saranno pure i periodi più ampii, aggregati dei periodi binarii, che avremo dovuto in precedenza determinare. Così tutte le successive risolventi saranno a radici reali e soltanto colla risoluzione dell'ultima equazione quadratica che, noto il periodo binario $\varepsilon+\varepsilon^{-1}$, dà la ε stessa, passeremo alle radici immaginarie della proposta.

§. 98. — Per applicare ad esempî effettivi i processi generali indicati nel §. precedente, prendiamo i casi

$$p = 5 \quad p = 17.$$

Se $p = 5$ i periodi binarii sono

$$\eta_0 = \varepsilon + \varepsilon^4, \quad \eta_1 = \varepsilon^2 + \varepsilon^3$$

e poichè

$$\eta_0 + \eta_1 = -1, \quad \eta_0 \eta_1 = -1,$$

si trova subito per la risolvente di 2.° grado

$$F_2(\eta) = \eta^2 + \eta - 1 = 0 \text{ [1]}.$$

Delle due radici una si può eguagliare a η_0 l'altra a η_1, poniamo

$$\eta_0 = \frac{-1+\sqrt{5}}{2}, \quad \eta_1 = \frac{-1-\sqrt{5}}{2}.$$

Trovato η_0, resta da risolversi l'equazione di 2.° grado

$$(x-\varepsilon)(x-\varepsilon^4) = x^2 - \eta_0 x + 1 = 0;$$

possiamo quindi porre

$$\varepsilon = \frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$

---

[1]) Questo caso del resto si può trattare indipendentemente dalla teoria generale, essendo l'equazione $x^4+x^3+x^2+x+1=0$ un'equazione reciproca.

Ove si assumano i radicali positivi, si vedrà subito che si ha $\varepsilon = \cos\frac{2\pi}{5} + i \operatorname{sen}\frac{2\pi}{5}$ e la formola

$$2\cos\frac{2\pi}{5} = \eta_0 = \frac{\sqrt{5}-1}{2}$$

consente una costruzione geometrica ben semplice del pentagono regolare iscritto [1]).

Prendendo ora $p = 17$ e scegliendo per radice primitiva $g = 3$, costruiamo anzi tutto la tabella d'indici

numero	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
indice	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

che ci dà la distribuzione delle radici in periodi e formiamo i periodi di 8 termini

$$\eta_0 = \varepsilon + \varepsilon^9 + \varepsilon^{13} + \varepsilon^{15} + \varepsilon^{16} + \varepsilon^8 + \varepsilon^4 + \varepsilon^2$$
$$\eta_1 = \varepsilon^3 + \varepsilon^{10} + \varepsilon^5 + \varepsilon^{11} + \varepsilon^{14} + \varepsilon^7 + \varepsilon^{12} + \varepsilon^6,$$

gli esponenti della ε in η_0 essendo i residui, in η_1 i non residui. Scindiamo poi η_0 in due periodi minori η'_0, η'_1 corrispondenti agli indici

$$0, 4, 8, 12 \quad \text{per } \eta'_0$$
$$2, 6, 10, 14 \quad \text{per } \eta'_2$$

e similmente η_1 nei due periodi η'_1, η'_3 corrispondenti agli indici

$$1, 5, 9, 13 \quad \text{per } \eta'_1$$
$$3, 7, 11, 15 \quad \text{per } \eta'_3;$$

poniamo cioè

$$\eta'_0 = \varepsilon + \varepsilon^{13} + \varepsilon^{16} + \varepsilon^4 \quad , \quad \eta'_2 = \varepsilon^9 + \varepsilon^{15} + \varepsilon^8 + \varepsilon^2$$
$$\eta'_1 = \varepsilon^3 + \varepsilon^5 + \varepsilon^{14} + \varepsilon^{12} \quad , \quad \eta'_3 = \varepsilon^{10} + \varepsilon^{11} + \varepsilon^7 + \varepsilon^6.$$

In fine scindiamo η'_0 nei periodi binarii

$$\eta''_0 = \varepsilon + \varepsilon^{16}$$
$$\eta''_4 = \varepsilon^{13} + \varepsilon^4.$$

---

[1]) Vedi *Bachmann Kreistheilung*, pag. 61.

Se, per fissare le idee, assumiamo

$$\varepsilon = \cos\frac{2\pi}{17} + i \operatorname{sen}\frac{2\pi}{17}$$

vediamo subito che i tre periodi

$$\eta_0 = 2\left(\cos\frac{2\pi}{17} + \cos\frac{4\pi}{17} + \cos\frac{8\pi}{17} + \cos\frac{16\pi}{17}\right)$$

$$\eta'_1 = 2\left(\cos\frac{6\pi}{17} + \cos\frac{10\pi}{17}\right)$$

$$\eta'_0 = 2\left(\cos\frac{2\pi}{17} + \cos\frac{8\pi}{17}\right)$$

sono positivi.

Ora per costruire la risolvente di 2.° grado di cui η_0, η_1 sono radici, basta osservare che si ha

$$\eta_0 + \eta_1 = -1 \ , \quad \eta_0\,\eta_1 = 4\,(\eta_0 + \eta_1) = -4 \ ,$$

onde la risolvente sarà

$$\eta^2 + \eta - 4 = 0$$

e ne risulterà

$$(\alpha) \qquad \eta_0 = \frac{\sqrt{17} - 1}{2} \ , \quad \eta_1 = -\frac{\sqrt{17} + 1}{2} \ .$$

Abbiamo poi

$$\eta'_0 + \eta'_2 = \eta_0 \ , \quad \eta'_0\,\eta'_2 = -1$$

$$\eta'_1 + \eta'_3 = \eta_1 \ , \quad \eta'_1\,\eta'_3 = -1$$

e per ciò η'_0, η'_2 sono le radici della equazione

$$\eta'^2 - \eta_0\,\eta' - 1 = 0$$

e η'_1, η'_3 quelle dell'altra

$$\eta'^2_a - \eta_1\,\eta' - 1 = 0 \ ,$$

donde ricaviamo

$$(\beta) \qquad \eta'_0 = \frac{\eta_0}{2} + \sqrt{\frac{\eta_0^2}{4} + 1} \ , \quad \eta'_1 = \frac{\eta_1}{2} + \sqrt{\frac{\eta_1^2}{4} + 1} \ ,$$

attribuendo ai radicali i segni positivi.

In fine essendo

$$\eta''_0 + \eta''_4 = \eta'_0 \quad , \quad \eta''_0 \eta''_4 = \eta'_1 ,$$

deduciamo

$$\eta''_0 = 2 \cos \frac{2\pi}{17} = \frac{\eta'_0}{2} + \sqrt{\frac{\eta'^2_0}{4} - \eta'_1} .$$

Sostituendo in questa per η'_0, η'_1 i valori (β), calcolati mediante la (α), costruiamo $2 \cos \frac{2\pi}{17}$. La interpretazione geometrica di questa formola dà la costruzione del poligono regolare di 17 lati [1]).

§. 99. — Ritorniamo alla equazione generale

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

per costruirne la risolvente di secondo grado che ha per radici i periodi di $\frac{p-1}{2}$ termini

$$\begin{cases} \eta_0 = \varepsilon + \varepsilon^{g^2} + \varepsilon^{g^4} + \ldots + \varepsilon^{g^{p-3}} \\ \eta_1 = \varepsilon^g + \varepsilon^{g^3} + \varepsilon^{g^5} + \ldots + \varepsilon^{g^{p-2}} . \end{cases}$$

Siccome conosciamo già

$$\eta_0 + \eta_1 = -1 ,$$

basterà calcolare il discriminante

$$\Delta = (\eta_0 - \eta_1)^2 .$$

Ora abbiamo

$$\eta_0 - \eta_1 = \sum \varepsilon^a - \sum \varepsilon^b ,$$

percorrendo a i residui quadratici e b i non residui (mod p), sicchè possiamo scrivere

$$\eta_0 - \eta_1 = \sum_{\mu} (-1)^{\operatorname{ind} \mu} \varepsilon^{\mu} ,$$

dove facciamo percorrere a μ un sistema completo di resti (mod p),

---

[1]) Cf. Bachmann, *l. c.*, pag. 66-68.

escluso lo zero; ne deduciamo:

$$(\eta_0 - \eta_1)^2 = \sum_{\nu} \left(\sum_{\mu} (-1)^{\operatorname{ind}\mu + \operatorname{ind}\nu} . \varepsilon^{\mu+\nu} \right) .$$

Ma poichè, restando fisso $\nu \not\equiv 0 \pmod{p}$, $\mu\nu$ percorre insieme con μ un sistema completo di resti, cangiando nella somma interna μ in $\mu\nu$, possiamo scrivere

$$\Delta = \sum_{\nu} \sum_{\mu} (-1)^{\operatorname{ind}\mu} \varepsilon^{\nu(\mu+1)},$$

ovvero, invertendo le sommazioni:

$$\Delta = \sum_{\mu=1}^{\mu=p-1} (-1)^{\operatorname{ind}\mu} \left\{ \varepsilon^{\mu+1} + \varepsilon^{2(\mu+1)} + \ldots + \varepsilon^{(p-1)(\mu+1)} \right\} .$$

Ora la somma $\varepsilon^{\mu+1} + \varepsilon^{2(\mu+1)} + \ldots + \varepsilon^{(p-1)(\mu+1)}$ è eguale a $p-1$ se $\mu \equiv -1 \pmod{p}$ ed è invece $= -1$ in tutti gli altri casi. Dunque si ha

$$\Delta = (-1)^{\operatorname{ind}(p-1)} . p - \sum_{\mu=1}^{\mu=p-1} (-1)^{\operatorname{ind}\mu},$$

ovvero, perchè la seconda somma è evidentemente nulla:

$$\Delta = (-1)^{\frac{p-1}{2}} p .$$

Essendo poi $(\eta_0 + \eta_1)^2 = 1$, avremo

$$\eta_0 \eta_1 = \frac{1 - (-1)^{\frac{p-1}{2}} p}{4} ;$$

quindi la cercata risolvente di 2.° grado è la seguente:

$$\eta^2 + \eta + \frac{1 - (-1)^{\frac{p-1}{2}} p}{4} = 0$$

ed ha per radici

$$\eta_0 = \frac{-1 + \sqrt{(-1)^{\frac{p-1}{2}} p}}{2} , \quad \eta_1 = \frac{-1 - \sqrt{(-1)^{\frac{p-1}{2}} p}}{2} .$$

Dai teoremi generali si ottiene quindi il notevole risultato:

L'equazione $x^{p-1}+x^{p-2}+\ldots+x+1=0$, *che è irriducibile nel campo assoluto di razionalità, diventa riducibile per l'aggiunta del radicale quadratico*

$$\sqrt{(-1)^{\frac{p-1}{2}}.p}$$

e si spezza in due fattori irriducibili di grado $\frac{p-1}{2}$ *ciascuno* [1]).

I coefficienti di questi fattori saranno funzioni lineari intere a coefficienti interi di η_0, η_1; i detti fattori avranno quindi la forma

$$\frac{Y(x)+Z(x)\sqrt{(-1)^{\frac{p-1}{2}}p}}{2}$$

$$\frac{Y(x)-Z(x)\sqrt{(-1)^{\frac{p-1}{2}}p}}{2},$$

dove $Y(x)$, $Z(x)$ sono polinomii a coefficienti interi. Ne risulta la formola notevole

$$4\,\frac{x^p-1}{x-1}=Y^2(x)-(-1)^{\frac{p-1}{2}}p\,Z^2(x).$$

---

[1]) La medesima cosa si vede anche calcolando il discriminante D della equazione $x^p-1=0$ che è dato dal determinante

$$D=\begin{vmatrix} s_0 & s_1 & s_2 & \ldots & s_{p-1} \\ s_1 & s_2 & s_3 & \ldots & s_p \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ s_{p-1} & s_p & s_{p+1} & \ldots & s_{2p-1} \end{vmatrix},$$

dove s_r indica la somma delle potenze r^{me} delle radici e siccome $s_r=0$ per $r\not\equiv 0 \pmod p$ mentre $s_p=p$ si ha

$$D=(-1)^{\frac{p-1}{2}}p^p.$$

Il discriminante Δ della $x^{p-1}+x^{p-2}+\ldots+x+1=0$ non differisce da D che pel quadrato del fattore

$$(1-\varepsilon)(1-\varepsilon^r)\ldots(1-\varepsilon^{p-1})=X_p(1)=p;$$

si ha precisamente $\Delta=\frac{D}{p^2}=(-1)^{\frac{p-1}{2}}p^{p-2}$. Aggiungendo al campo di razionalità $\sqrt{\Delta}$, cioè $\sqrt{(-1)^{\frac{p-1}{2}}p}$, il gruppo della $X_p(x)=0$ si riduce al sottogruppo d'indice 2 delle sostituzioni pari.

§. 100. — Dalla formola

$$(\eta_0 - \eta_1)^2 = (-1)^{\frac{p-1}{2}} p$$

sopra stabilita può dedursi un' elegante dimostrazione della legge di reciprocità nella teoria dei residui quadratici, che è la sesta dimostrazione di Gauss.

Posto

$$S = \eta_0 - \eta_1 = \sum_r \left(\frac{r}{p}\right) \varepsilon^r,$$

dove r percorre un sistema completo di resti (mod p), escluso lo zero, ed $\left(\frac{r}{p}\right)$ è il simbolo di Legendre, abbiamo

$$S^2 = (-1)^{\frac{p-1}{2}} p.$$

Ora sia q un altro numero primo impari; elevando quest'ultima formola alla potenze $\frac{q-1}{2}$, indi moltiplicandola per S, abbiamo

$$S^q = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} p^{\frac{q-1}{2}} S$$

da cui

$$(a) \qquad S^q - \left(\frac{q}{p}\right) S = \left\{ (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right) \right\} S.$$

Ma si ha

$$\left(\frac{q}{p}\right) S = \sum_r \left(\frac{qr}{p}\right) \varepsilon^r$$

e, poichè qr percorre un sistema completo di resti insieme con r, potremo cangiare nel segno sommatorio r in qr, il che dà:

$$\left(\frac{q}{p}\right) S = \sum_r \left(\frac{r}{p}\right) \varepsilon^{qr}.$$

La formola (a) può quindi scriversi

$$\left[\sum \left(\frac{r}{p}\right) \varepsilon^r\right]^q - \sum \left(\frac{r}{p}\right) \varepsilon^{qr} = \left\{ (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right) \right\} \cdot \sum_{r=1}^{r=p-1} \left(\frac{r}{p}\right) \varepsilon^r$$

e riducendo gli esponenti di ε nel primo membro ai loro minimi resti positivi (mod p), dovranno risultare i coefficienti delle medesime potenze

di ε eguali dalle due parti, a causa della irriducibilità dell'equazione fondamentale. Ora essendo

$$\left(\frac{r}{p}\right)^q = \left(\frac{r}{p}\right),$$

le potenze q^{me} dei termini della somma $\sum\left(\frac{r}{p}\right)\varepsilon^r$ vengono distrutte dai termini della seconda somma e tutti i rimanenti coefficienti rimangono dunque divisibili per q; avremo quindi la congruenza

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{q}.$$

D'altra parte si ha pel teorema d'Eulero

$$p^{\frac{p-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod{q};$$

dunque risulta la formola

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

che è la ben nota espressione del teorema di reciprocità.

§. 101. — Abbiamo già osservato (§. 96) che la risolvente (12)

$$F_e(\eta) = 0$$

si risolve coll'estrazione di un radicale d'indice $e\sqrt[e]{B}$, che porta sopra una quantità razionalmente composta colla radice α primitiva, d'ordine e, dell'unità. Ora ci proponiamo di costruire effettivamente la quantità B sotto il segno radicale, ciò che conduce a conseguenze aritmetiche di molto interesse.

Faremo dapprima il calcolo sulla proposta stessa

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0, \tag{14}$$

corrispondente al valore $p-1$ di e e dai risultati così ottenuti seguiranno subito quelli relativi alla risolvente $F_e(\eta) = 0$.

Secondo il metodo generale (§. 74) per la risoluzione di un'equazione Abeliana a gruppo ciclico, indicando con

$$x_0 = \varepsilon\,,\quad x_1 = \varepsilon^g\,,\quad x_2 = \varepsilon^{g^2}\,,\ \ldots\ x_{p-2} = \varepsilon^{g^{p-2}}$$

le radici delle (14) distribuite in un unico periodo e con ω una radice primitiva della equazione $x^{p-1} = 1$, dobbiamo a quest'oggetto costruire la funzione razionale delle radici:

$$\varepsilon + \omega^h \varepsilon^g + \omega^{2h} \varepsilon^{g^2} + \ldots + \omega^{(p-2)h} \varepsilon^{g^{p-2}}\,,$$

che indicheremo, come al §. 74, col simbolo

$$(\omega^h, \varepsilon) = \sum_{\lambda=0}^{\lambda=p-2} \omega^{h\lambda} \varepsilon^{g^\lambda}\,. \tag{15}$$

In generale la (ω^h, ε) sarà razionalmente esprimibile per la (ω, ε) e la $(p-1)^{\text{ma}}$ potenza di (ω, ε) sarà razionalmente nota dopo l'aggiunta di ω; per calcolare ε avremo indi la formola

$$\varepsilon = \frac{1}{p-1}\left\{(1, \varepsilon) + (\omega, \varepsilon) + (\omega^2, \varepsilon) + \ldots + (\omega^{p-2}, \varepsilon)\right\}. \tag{16}$$

Dalle (15) si forma poi subito la corrispondente espressione risolvente per la $F_e(\eta) = 0$.

Basta farvi per ciò

$$h = rf \quad (r = 0,\ 1,\ 2 \ldots e-1),$$

con che si ottiene

$$(\omega^{rf}, \varepsilon) = \eta_0 + \omega^{rf} \eta_1 + \omega^{2rf} \eta_2 + \ldots + \omega^{(e-1)rf} \eta_{e-1}\,,$$

ossia, poichè $\omega^f = \alpha$ è una radice primitiva della $x^e = 1$, l'espressione

$$(\alpha^r, \eta_0) = \eta_0 + \alpha^r \eta_1 + \alpha^{2r} \eta_2 + \ldots + \alpha^{(e-1)r} \eta_{e-1}\,, \tag{17}$$

formata nel modo del §. 74 colle radici di $F_e(\eta) = 0$ e colla radice α d'ordine e dell'unità.

Ora si tratta dunque di esprimere effettivamente (ω^h, ε) $h = 2, 3 \ldots p-2$ razionalmente per (ω, ε) e la potenza $(\omega, \varepsilon)^{p-1}$ per ω, come analogamente (α^r, η_0) per (α, η_0) e la potenza $(\alpha, \eta_0)^e$ per α.

§. 102. — Prendendo la radice primitiva g (mod p) per base di un sistema d'indici, la (15) può scriversi [1]):

$$(\omega^h, \varepsilon) = \sum_{\mu=1}^{\mu=p-1} \omega^{h \operatorname{ind} \mu} \varepsilon^{\mu} .$$

Cangiando in questa ε in ε^{ν}, essendo $\nu \not\equiv 0$ (mod p), abbiamo

$$(\omega^h, \varepsilon^{\nu}) = \sum_{\mu=1}^{\mu=p-1} \omega^{h \operatorname{ind} \mu} \varepsilon^{\mu\nu}$$

e, poichè $\mu\nu$ percorre con μ un sistema completo di resti (zero escluso), possiamo scrivere

$$(18) \qquad (\omega^h, \varepsilon^{\nu}) = \omega^{-h \operatorname{ind} \nu} \sum_{\mu=1}^{\mu=p-1} \omega^{h \operatorname{ind} \mu} \varepsilon^{\mu},$$

il che dà la formola fondamentale

$$(A) \qquad (\omega^h, \varepsilon^{\nu}) = \omega^{-h \operatorname{ind} \nu} (\omega^h, \varepsilon).$$

Ora prendiamo due espressioni

$$(\omega^h, \varepsilon) \quad , \quad (\omega^k, \varepsilon)$$

e moltiplichiamole fra loro; avremo

$$(\omega^h, \varepsilon)\,(\omega^k, \varepsilon) = \sum_{\mu} \sum_{\nu} \omega^{h \operatorname{ind} \mu + k \operatorname{ind} \nu} \varepsilon^{\mu+\nu},$$

percorrendo sì μ che ν un sistema completo di resti, con esclusione dello zero. Nella sommazione rispetto a ν, restando fisso μ, cangiamo ν in $\mu\nu$ ed otterremo

$$(\omega^h, \varepsilon)\,(\omega^k, \varepsilon) = \sum_{\mu} \sum_{\nu} \omega^{(h+k) \operatorname{ind} \mu + k \operatorname{ind} \nu} . \varepsilon^{\mu(\nu+1)},$$

---

[1]) Pei calcoli seguenti si ritenga presente che l'eguaglianza $\varepsilon^r = \varepsilon^s$ equivale alla congruenza $r \equiv s$ (mod p), come l'altra $\omega^h = \omega^k$ alla congruenza $h \equiv k$ (mod $p-1$).

che, invertendo le sommazioni, potremo scrivere

$$(19) \qquad (\omega^h, \varepsilon)(\omega^k, \varepsilon) = \sum_{\nu=1}^{\nu=p-1} \omega^{k \operatorname{ind} \nu} \sum_{\mu=1}^{\mu=p-1} \omega^{(h+k) \operatorname{ind} \mu} \cdot \varepsilon^{\mu(\nu+1)}.$$

Ed ora distinguiamo due casi secondo che

$$h + k \not\equiv 0 \pmod{p-1},$$

ovvero

$$h + k \equiv 0 \pmod{p-1}.$$

1.° caso — Se $h+k \not\equiv 0 \pmod{p-1}$, la sommazione rispetto a μ pei valori di ν

$$\nu = 1, 2, 3 \ldots p-2$$

dà per la (18) e per la (A)

$$\sum_{\mu=1}^{\mu=p-1} \omega^{(h+k) \operatorname{ind} \mu} \varepsilon^{(\mu\nu+1)} = (\omega^{h+k}, \varepsilon^{\nu+1}) = \omega^{-(h+k) \operatorname{ind} (\nu+1)} (\omega^{h+k}, \varepsilon),$$

mentre per $\nu = p-1$ si ha

$$\sum_{\mu=1}^{\mu=p-1} \omega^{(h+k) \operatorname{ind} \mu} = 0,$$

onde la (19) diventa

$$(\omega^h, \varepsilon)(\omega^k, \varepsilon) = (\omega^{h+k}, \varepsilon) \sum_{\nu=1}^{\nu=p-2} \omega^{k \operatorname{ind} \nu - (h+k) \operatorname{ind} (\nu+1)}.$$

Si ha dunque la formola:

$$(B) \quad \frac{(\omega^h, \varepsilon)(\omega^k, \varepsilon)}{(\omega^{h+k}, \varepsilon)} = \sum_{\nu=1}^{\nu=p-2} \omega^{k \operatorname{ind} \nu - (h+k) \operatorname{ind} (\nu+1)} \text{ per } h+k \not\equiv 0 \bmod p-1),$$

che, in ragione della simmetria del primo membro rispetto ad h, k, si può scrivere in un secondo modo, scambiando h con k.

Il secondo membro della (B) è evidentemente della forma

$$c_0 + c_1 \omega + c_2 \omega^2 + \ldots + c_{p-2} \omega^{p-2},$$

con c numeri razionali interi; esso è un *numero intero algebrico* nel campo $(1, \omega)$.

2.° caso — Sia ora $h+k \equiv 0 \pmod{p-1}$. Allora la (19) diventa

$$(\omega^h, \varepsilon)\,(\omega^{-h}, \varepsilon) = \sum_{\nu=1}^{\nu=p-1} \omega^{-h \operatorname{ind} \nu} \sum_{\mu=1}^{\mu=p-1} \varepsilon^{\mu(\nu+1)};$$

ma si ha

$$\sum_{\mu=1}^{\mu=p-1} \varepsilon^{\mu(\nu+1)} = -1 \quad \text{per } \nu = 1, 2, 3, \ldots p-2$$

e invece

$$\sum_{\mu=1}^{\mu=p-1} \varepsilon^{\mu p} = p-1 \quad (\nu = p-1),$$

da cui

$$(\omega^h, \varepsilon)\,(\omega^{-h}, \varepsilon) = \omega^{-h \operatorname{ind}(p-1)}\, p - \sum_{\nu=1}^{\nu=p-1} \omega^{-h \operatorname{ind} \nu}.$$

Ora abbiamo $\operatorname{ind}(p-1) = \frac{p-1}{2}$ e, se $h \not\equiv 0 \pmod{p-1}$, è

$$\sum_{\nu=1}^{\nu=p-1} \omega^{-h \operatorname{ind} \nu} = 0;$$

risulta quindi la formola

$$\text{(C)} \qquad (\omega^h, \varepsilon)\,(\omega^{-h}, \varepsilon) = (-1)^h\, p \qquad (h \not\equiv 0 \pmod{p-1}),$$

che è da sostituirsi alla (B) per $h+k \equiv 0 \pmod{p-1}$.

La (C) ci dimostra intanto che *nessuna delle espressioni* (ω^h, ε) *si annulla*, ciò che è ben necessario osservare perchè non risulti dubbia l'applicabilità dei metodi generali per le equazioni Abeliane (Cf. §§. 78, 79).

§. 103. — Le formole fondamentali (B) (C) conducono con facilità a risolvere la questione posta nel §. 101. Dalla (B) fattovi

$$k = n\,h$$

e supposto che dei tre numeri interi

$$h\,,\ n\,h\,,\ (n+1)\,h$$

non ve ne sia alcuno divisibile per $p-1$, avremo

$$\text{(20)} \qquad (\omega^h, \varepsilon)\,(\omega^{nh}, \varepsilon) = (\omega^{(n+1)h}, \varepsilon)\,\psi_n(\omega^h),$$

ove si ponga per brevità

$$(21) \qquad \psi_n(\omega^h) = \sum_{\mu=1}^{\mu=p-2} (\omega^h)^{\operatorname{ind}\mu-(n+1)\operatorname{ind}(\mu+1)} ;$$

questa quantità $\psi_n(\omega^h)$ viene quindi ad essere un intero algebrico nel campo $(1, \omega^h)$.

Supposto ora che fra i numeri

$$h\ ,\ 2h\ ,\ 3h\ ,\ \ldots\ mh$$

non ve ne sia alcuno divisibile per $p-1$, potremo fare successivamente nella (20)

$$n = 1\ ,\ 2\ ,\ 3 \ldots m-1$$

e moltiplicando tutte queste relazioni fra loro, col togliere i fattori comuni (non nulli) comuni alle due parti, avremo

$$(22) \qquad (\omega^h, \varepsilon)^m = (\omega^{mh}, \varepsilon)\ \psi_1(\omega^h)\ \psi_2(\omega^h) \ldots \psi_{m-1}(\omega^h).$$

Facendo qui $h=1$, possiamo prendere

$$m = 1\ ,\ 2\ ,\ 3 \ldots p-2$$

e la (22) diventa

$$(D) \qquad (\omega, \varepsilon)^m = (\omega^m, \varepsilon)\ .\ \psi_1(\omega)\ \psi_2(\omega) \ldots \psi_{m-1}(\omega)\ ,$$

colla quale formola esprimiamo, come si voleva,

$$(\omega^2, \varepsilon)\ ,\ (\omega^3, \varepsilon)\ ,\ \ldots\ (\omega^{p-2}, \varepsilon)$$

razionalmente per (ω, ε). In fine per esprimere $(\omega, \varepsilon)^{p-1}$ razionalmente per ω deduciamo dalla (D) per $m = p-2$

$$(\omega, \varepsilon)^{p-2} = (\omega^{p-2}, \varepsilon)\ \psi_1(\omega)\ \psi_2(\omega) \ldots \psi_{p-3}(\omega)\ ,$$

indi dalla (C) per $h=1$

$$(\omega, \varepsilon)\ (\omega^{p-2}, \varepsilon) = -p\ ,$$

che, moltiplicata per la precedente, ci dà la formola finale richiesta:

$$(E) \qquad (\omega, \varepsilon)^{p-1} = -p\ \psi_1(\omega)\ \psi_2(\omega)\ \psi_3(\omega) \ldots \psi_{p-3}(\omega)\ .$$

Per ottenere poi le formole analoghe per la risolvente $F_e(\eta) = 0$, facciamo nella (22) $h = f$, indi $\omega^h = \alpha$, e purchè si prenda m nella serie

$$1, 2, 3, \ldots e - 1$$

potremo, per quanto precede, applicare la (22), il che ci dà:

$$(F) \qquad (\alpha, \eta_0)^m = (\alpha^m, \eta_0)\, \psi_1(\alpha)\, \psi_2(\alpha) \ldots \psi_{m-1}(\alpha),$$

essendo $\psi_n(\alpha)$ un numero complesso intero nel campo $(1, \alpha)$ definito dalla formola

$$(23) \qquad \psi_n(\alpha) = \sum_{\mu=1}^{\mu=p-2} \alpha^{\text{ind}\,\mu - (n+1)\,\text{ind}\,(\mu+1)}.$$

Se osserviamo poi che la (C) per $h = f$ dà

$$(\alpha, \eta_0)(\alpha^{-1}, \eta_0) = (-1)^f . p$$

e la (F) per $m = e - 1$ diventa

$$(\alpha, \eta_0)^{e-1} = (\alpha^{e-1}, \eta_0)\, \psi_1(\alpha)\, \psi_2(\alpha) \ldots \psi_{e-2}(\alpha),$$

moltiplicando le due ultime fra loro deduciamo

$$(G) \qquad (\alpha, \eta_0)^e = (-1)^f . p\, \psi_1(\alpha)\, \psi_2(\alpha) \ldots \psi_{e-2}(\alpha).$$

Questa, insieme colla (E), risolve completamente per la $F_e(\eta) = 0$, la questione proposta.

§. 104. — Nelle formole di risoluzione delle equazioni della divisione del circolo abbiamo visto introdursi i numeri complessi interi $\psi_n(\alpha)$ del campo $(1, \alpha)$. Ci è impossibile qui trattenerci sulla teoria generale di questi numeri complessi pei quali Kummer pel primo, colla sua creazione dei numeri ideali, ha costruita una teoria affatto analoga a quella degli ordinari numeri razionali interi. Solo ci contenteremo dimostrare come, colle formole del §. precedente, si possa effettuare una decomposizione di ogni numero primo $p \equiv 1 \pmod{e}$ nel prodotto di due numeri complessi interi nel campo $(1, \alpha)$.

Supposto che dei tre numeri

$$h,\ k,\ h+k$$

non ve ne sia alcuno divisibile per $p-1$, dalla (B) abbiamo

$$\frac{(\omega^h,\ \varepsilon)\ (\omega^k,\ \varepsilon)}{\omega^{h+k},\ \varepsilon} = \sum_{\mu=1}^{\mu=p-2} \omega^{h \text{ ind } \mu - (h+k) \text{ ind } (\mu+1)}$$

ed anche

$$\frac{(\omega^{-h},\ \varepsilon)\ (\omega^{-k},\ \varepsilon)}{(\omega^{-(h+k)},\ \varepsilon)} = \sum_{\mu=1}^{\mu=p-2} \omega^{-h \text{ ind } \mu + (h+k) \text{ ind } (\mu+1)}\ .$$

Moltiplicando queste due formule, coll'osservare la (C), si ottiene:

$$p = \sum_{\mu=1}^{\mu=p-2} \omega^{h \text{ ind } \mu - (h+k) \text{ ind } (\mu+1)} \cdot \sum_{\mu=1}^{\mu=p-2} \omega^{-h \text{ ind } \mu + (h+k) \text{ ind } (\mu+1)}\ .$$

E facendo ora, come è lecito

$$h = f\ ,\ \ k = (e-2)f\ ,$$

avremo la formola:

$$(24) \qquad p = \sum_{\mu=1}^{\mu=p-2} \alpha^{\text{ind } \mu + \text{ind } (\mu+1)} \cdot \sum_{\mu=1}^{\mu=p-2} \alpha^{-\text{ind } \mu - \text{ind } (\mu+1)}\ ,$$

che dà la decomposizione di p nel prodotto di due due numeri interi complessi *coniugati* nel campo $(1,\ \alpha)$.

Se, come caso particolare, facciamo $e = 4$ indi $\alpha = \sqrt{-1} = i$ la (24) ci dà la decomposizione di $p \equiv 1 \pmod{4}$ nel prodotto di due numeri complessi coniugati di Gauss

$$p = (a+bi)\ (a-bi) = a^2 + b^2,$$

essendo a, b interi ordinarii. Ne risulta il teorema di Fermat:

Ogni numero primo della forma $4n+1$ *è la somma di due quadrati.*

CAPITOLO VIII.

Equazioni con un parametro. — Gruppo di monodromia. — Equazioni dei poliedri regolari. L'irrazionalità icosaedrica e la risoluzione della equazione generale di 5.° grado secondo KLEIN.

§. 105. — Le equazioni a cui fin qui abbiamo applicato le teorie generali di GALOIS avevano per coefficienti costanti assolute. Ma le teorie stesse sono egualmente applicabili al caso in cui i cofficienti della proposta contengono un parametro arbitrario. Le più importanti equazioni che ci fornisce l'analisi, come le equazioni per la divisione dell'argomento nelle funzioni circolari ed ellittiche, le equazioni per la trasformazione delle funzioni ellittiche, le equazioni modulari ecc. appartengono appunto a questa categoria.

Importa quindi che ci occupiamo della teoria di queste equazioni dal punto di vista di GALOIS. Indichiamo con x l'incognita della nostra equazione e con t il parametro, che supponiamo entrare razionalmente nei coefficienti; l'equazione si potrà scrivere

$$f(x, t) = 0, \tag{1}$$

ove f è il simbolo di una funzione razionale intera nelle due variabili x, t.

Ordinando per le potenze di x e supponendo che la (1) sia di grado m in x, questa si scriverà

$$a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = 0, \tag{1*}$$

dove le a sono polinomii razionali interi in t con coefficienti appartenenti ad un dato campo di razionalità

$$(\mathrm{R}, \mathrm{R}', \mathrm{R}'' \ldots).$$

Ad ogni valore reale o complesso di t corrisponderanno *in generale* m valori finiti di x e cioè le m radici

$$x_1, x_2 \ldots x_m$$

della (1*). Soltanto per quei valori speciali di t che annullano a_0 si pre-

senta un caso d'eccezione in quanto che la (1) offre allora una o più radici infinite [1]).

Questo caso può sempre evitarsi operando la trasformazione $y = a_0 x$; la nuova equazione in y avrà il primo coefficiente $= 1$ e gli altri polinomii razionali interi in t.

Se aggiungiamo al campo di razionalità (R, R′, R″...) il parametro o indeterminata t, e riguardiamo quindi come razionalmente nota ogni funzione razionale di t con coefficienti appartenenti al campo (R, R′, R″...), riprendendo le considerazioni fondamentali, che ai §§. 61-64 ci hanno condotto al concetto di *gruppo di* Galois per l'equazione, facilmente vediamo che esse rimangono ancora applicabili. Potremo infatti costruire ancora la risolvente di Galois, che conterrà nei suoi coefficienti razionalmente t, ed esaminarne lo spezzamento in fattori irriducibili, che dovranno essere funzioni razionali intere di Y, t con coefficienti razionali nel campo (R, R′, R″...)

Il gruppo di Galois G per l'equazione (1*) nel campo (R, R′, R″...), ampliato coll'aggiunta dell'indeterminata t, si dirà il *gruppo algebrico* della equazione nel campo (R, R′, R″...) per distinguerlo dal così detto gruppo di monodromia, del quale ora tratteremo.

Enunciamo le proprietà fondamentali del gruppo algebrico, come risultano immediatamente dai teoremi del §. 65:

1.ª Se una funzione razionale $\varphi(x_1, x_2 \ldots x_m, t)$ delle m radici della (1) e del parametro t *con coefficienti razionali nel campo* (R, R′, R″...) rimane invariata per tutte le sostituzioni di G, essa è una funzione razionale di t *con coefficienti razionali in* (R, R′, R″...).

2.ª Inversamente se la funzione razionale $\varphi(x_1, x_2 \ldots x_m, t)$ di $x_1, x_2 \ldots x_m$ e di t *con coefficienti razionali* è una funzione razionale di t *con coefficienti razionali*, essa rimane invariata per qualunque sostituzione del gruppo algebrico sulle x.

§. 106. — Per lo studio delle equazioni con un parametro ha la massima importanza il *gruppo di monodromia* dell'equazione, che definiamo dapprima nel modo seguente:

---

(1) Diventeranno precisamente infinite r radici se il valore considerato $t = t_0$ annullerà

$$a_0, a_1, a_2 \ldots a_{r-1}$$

senza annullare a_r.

Diciamo gruppo di monodromia della equazione (1) *il gruppo algebrico che l'equazione acquista quando per campo di razionalità si assuma quello di tutte le quantità costanti.*

Le proprietà fondamentali del gruppo Γ di monodromia si deducono da quelle sopra enunciate pel gruppo algebrico G, omettendo la condizione che le funzioni da considerarsi abbiano coefficienti razionali, poichè attualmente ogni quantità costante si riguarda come razionalmente nota. Abbiamo così i teoremi:

1.° *Ogni funzione razionale delle radici della* (1) *e del parametro t, che rimanga invariata per tutte le sostituzioni del gruppo Γ di monodromia, è esprimibile come funzione razionale di t.*

2.° *Inversamente, se una funzione razionale di $x_1, x_2 \ldots x_m$ e di t è razionalmente esprimibile per la sola t, essa resta invariata per qualunque sostituzione del gruppo Γ di monodromia.*

Queste proprietà sono poi caratteristiche del gruppo di monodromia e cioè vale il teorema:

Se una sostituzione sulle x lascia invariata qualunque funzione razionale delle x e di t, che sia razionalmente esprimibile per t, essa appartiene al gruppo Γ di monodromia.

È bene evidente che il gruppo Γ di monodromia è in ogni caso un sottogruppo del gruppo algebrico G. Ora vogliamo dimostrare una proprietà di grande importanza e cioè che per ridurre il gruppo algebrico al gruppo di monodromia non importa ampliare il campo (R, R′, R″ . . .) a quello di tutte le quantità costanti, ma basta l'aggiunta *di un'unica irrazionalità numerica* α, radice di un'equazione normale

$$\varphi(\alpha) = 0\,,$$

con coefficienti razionali in (R, R′ R″. . .). Ne segue allora il teorema:

Il gruppo Γ di monodromia è in ogni caso sottogruppo invariante del gruppo algebrico G.

§. 107. — Per dimostrare il teorema enunciato, prendiamo una funzione razionale delle x e di t

$$y = \psi(x_1, x_2 \ldots x_m, t)$$

con coefficienti razionali in (R, R′, R″ . . .), che rimanga invariata per tutte

e sole le sostituzioni del gruppo Γ di monodromia e con questa costruiamo la risolvente

$$\Phi(y, t) = 0 \tag{3}$$

della proposta (1). Essendo la y invariabile per le sostituzioni di Γ, sarà esprimibile razionalmente per t, poniamo:

$$y = \theta(t).$$

Immaginiamo al posto dei coefficienti nella θ sostituite altrettante indeterminate

$$\beta_1, \beta_2 \ldots \beta_r$$

e sostituito questo valore di y nella (4). Riducendo intera l'equazione così ottenuta ed eguagliando a zero i coefficienti delle varie potenze di t, si avrà un certo numero di equazioni *con coefficienti razionali* per determinare $\beta_1, \beta_2 \ldots \beta_r$. Queste equazioni nelle β sono certamente compatibili (poichè esiste una determinata funzione $\theta(t) = y$ che soddisfa la (3)) nè possono essere insufficienti, cioè lasciare qualcuna delle β indeterminate; altrimenti la (3) sarebbe soddisfatta da infinite funzioni razionali di t, ciò che è assurdo. Dunque è possibile, presa una delle β, eliminare le rimanenti da queste equazioni e però ciascuna β_i è un irrazionale numerico, definito da un'equazione irriducibile

$$F_i(\beta) = 0$$

con coefficienti razionali in $(R, R', R'' \ldots)$. Considerando l'equazione che si ottiene facendo il prodotto dei primi membri delle F_i differenti, avremo un'equazione a radici diseguali di cui potremo costruire la risolvente di Galois e basterà conoscere una radice α di questa per conoscere anche tutte le β. L'aggiunta di α al campo di razionalità fa scendere il gruppo algebrico dell'equazione almeno fino a Γ perchè, dopo l'aggiunta di α, la y è razionalmente nota per t. D'altronde è impossibile che per tale aggiunta G scenda ad un puro sottogruppo di Γ, poichè persino nel massimo campo di razionalità, formato da tutte le quantità costanti, il gruppo algebrico dell'equazione è Γ. Ora, siccome α è radice di un'equazione normale, dal teorema al §. 79 segue che Γ è un sottogruppo invariante di G. Si ha dunque il teorema:

Il gruppo Γ *di monodromia di un'equazione ad un parametro è sempre sottogruppo invariante del suo gruppo algebrico* G; *per ridurre* G *a* Γ *basta*

aggiungere al campo di razionalità una sola irrazionalità numerica α, radice di un'equazione normale.

A questi risultati fondamentali aggiungiamo le osservazioni seguenti. Se il gruppo di monodromia Γ è transitivo, la proposta (1) è *irriducibile* nel senso che è impossibile scindere $f(x, t)$ nel prodotto di due fattori $\varphi(x, t) \,.\, \psi(x, t)$ razionali in x, t con coefficienti qualsiasi.

La transitività del gruppo algebrico assicura soltanto che una tale decomposizione è impossibile *se* $\varphi(x, t)$, $\psi(x, t)$ *debbono avere coefficienti razionali.*

Dicendo che la funzione razionale intera $f(x, t)$ delle due variabili x, t è irriducibile, intenderemo sempre che l'irriducibilità abbia luogo nel primo senso, che cioè il gruppo di monodromia sia transitivo. Ove si interpretino x, t come coordinate cartesiane correnti di un punto in un piano, ciò significa che la curva $f(x, t) = 0$ non si scinde in curve di grado minore.

§. 108. — Per fissare il concetto e stabilire le proprietà fondamentali del gruppo di monodromia ci siamo valsi, nei §§. precedenti, di considerazioni puramente algebriche.

Ma, per bene intendere la natura di questo gruppo, è necessario valersi anche di considerazioni che appartengono alla *teoria delle funzioni* (algebriche). E ciò è tanto più indispensabile che per le equazioni ad un parametro fornite dall'analisi la determinazione del gruppo di monodromia riesce appunto per considerazioni di questa natura. Ci limiteremo qui del resto a poche nozioni fondamentali.

Le m radici $x_1, x_2 \ldots x_m$ della $f(x, t) = 0$ hanno per ogni valore di t ciascuna un valore e sono funzioni della variabile complessa t. Quando la proposta è irriducibile (gruppo di monodromia transitivo) esse sono propriamente *gli m rami di una medesima funzione analitica x di t, che dicesi una funzione algebrica di t.* In generale, per un valore assegnato di t, i valori degli m rami sono distinti; coincidono invece due o più rami quando per la coppia considerata di valori di x, t si annulla insieme a $f(x, t)$, la sua derivata rispetto alla x. Eliminando la x fra le due equazioni

$$f(x, t) = 0 \,, \quad \frac{\partial f(x, t)}{\partial x} = 0 \,,$$

si avrà un'equazione risultante in t

$$F(t) = 0 \tag{4}$$

(discriminante), le cui radici saranno tutti e soli quei valori di t pei quali alcuni rami della funzione algebrica x vengono a coincidere. Immaginando i valori di t distesi sul piano complesso, ovvero sulla sfera complessa, i punti di questo piano (in numero finito) che sono indici delle radici della (4) diconsi i punti *critici* della funzione algebrica. Altri punti critici non abbiamo qui da considerare se, come supponiamo d'aver fatto con una previa trasformazione già indicata al §. 105, nella (1*) abbiamo ridotto il primo coefficiente a_0 ad una costante e gli altri a polinomii razionali interi in t. Supponiamo ora che l'indice di t parta da un punto A del piano complesso e vada ad un altro punto B per un cammino qualsiasi A C B *senza passare per alcun punto critico.*

In ogni punto del cammino A C B gli m rami sono distinti e se partiamo da A con uno determinato dei rami e lungo il cammino scegliamo sempre per x quel valore che succede per legge di continuità ai valori scelti nel cammino anteriore, non vi sarà mai ambiguità ed arriveremo in B con un valore perfettamente determinato per x, che sarà uno degli m valori della x in B.

Poniamo ora che partendo da A si descriva un cammino chiuso K, comunque intrecciato, che ritorni in A senza passare però per alcun punto critico. Se al principio abbiamo scelto in A uno dei rami, p. e. x_1, continuandolo lungo il cammino K secondo l'accennata legge di continuità, ritorneremo in A ancora con uno degli m valori che la x ha in A, che però potrà essere diverso da x_1, sia x_{i_1}. È chiaro che due rami diversi x_1, x_2 daranno al ritorno in A, lungo il medesimo cammino K, due rami x_{i_1}, x_{i_2} pure diversi; altrimenti, retrocedendo lungo K, i due rami coincidenti $x_{i_1} = x_{i_2}$ sarebbero cangiati con legge continua in rami diversi x_1, x_2, ciò che è assurdo. Così adunque l'effetto d'ogni cammino chiuso K sugli m rami

$$x_1 \; x_2 \ldots x_m$$

sarà di cangiarli negli m rami stessi

$$x_{i_1} \; x_{i_2} \ldots x_{i_m}$$

presi in altro ordine cioè: *Ogni cammino chiuso* K *produce sugli m rami una sostituzione*

$$\gamma = \begin{pmatrix} x_{i_1} & x_{i_2} & \dots & x_{i_m} \\ x_1 & x_2 & \dots & x_m \end{pmatrix}$$

È chiaro che invertendo il senso secondo cui il cammino K è percorso, il nuovo cammino, che indicheremo con K^{-1}, produrrà precisamente la sostituzione inversa γ^{-1}. E se i cammini K, K′ producono rispettivamente le sostituzioni γ, γ', il cammino K K′ composto che risulta dal percorrere, nel senso dovuto, prima K poi K′ produrrà la sostituzione composta $\gamma\,\gamma'$. Naturalmente la sostituzione prodotta da un determinato cammino chiuso K può anche essere l'identità. Ciò premesso, consideriamo tutti gli infiniti cammini chiusi che partono da A e vi ritornano; otterremo un numero (certamente finito, al massimo $= \pi(m)$) di sostituzioni

$$\gamma_1\,,\ \gamma_2 \dots \gamma_n$$

sugli m rami. Vediamo subito che: *Queste n sostituzioni* γ *formano un gruppo* Λ. E invero se i cammini chiusi K_i K_r producono le sostituzioni γ_i, γ_r il cammino composto $K_i\,K_r$ produce la sostituzione composta $\gamma_i\,\gamma_r$, che è dunque in Λ.

§. 109. — Ed ora, appoggiandosi sui principi della teoria delle funzioni, è ben facile dimostrare il teorema:

Il gruppo Λ *delle sostituzioni* γ_1, $\gamma_2 \dots \gamma_n$ *che si producono sugli m rami della funzione algebrica per tutti i possibili cammini chiusi che partono dal punto fissato* A *e vi ritornano, coincide col gruppo* Γ *di monodromia.*

In primo luogo, per dimostrare che ogni sostituzione γ_i di Λ appartiene a Γ, basta provare che γ_i lascia invariata *qualunque* funzione razionale $\varphi(x_1, x_2 \dots x_m t)$ degli m rami e di t che sia razionale in t. E invero avendosi

$$\varphi(x_1, x_2 \dots x_m, t) = F(t),$$

con F razionale in t, per i principii della teoria delle funzioni, la relazione precedente continuerà a verificarsi lungo tutto il cammino K_i che produce la $\gamma_i = \begin{pmatrix} x_{i_1} & x_{i_2} & \dots & x_{i_m} \\ x_1 & x_2 & \dots & x_m \end{pmatrix}$; ma al ritorno in A la F (t) riprende il

medesimo valore, dunque

$$\varphi(x_{i_1}, x_{i_2}, \ldots x_{i_m}, t) = \varphi(x_1 x_2, \ldots x_m, t) \quad \text{c. d. d.}$$

Per dimostrare poi inversamente che ogni sostituzione del gruppo di monodromia Γ appartiene a Λ conviene ricorrere al teorema della teoria delle funzioni che dice: *Ogni funzione algebrica di t che per qualunque cammino chiuso descritto da t ritorni col medesimo valore (sia monodroma) è necessariamente una funzione razionale di t.*

Ammessa questa proposizione, prendiamo una funzione razionale

$$\psi = \psi(x_1, x_2 \ldots x_m, t)$$

invariabile *per tutte e sole* le sostituzioni di Λ; essa è certamente una funzione algebrica di t, come radice di una risolvente della proposta, e poichè per ogni cammino chiuso la ψ, restando invariata per tutte le sostituzioni di Λ, riprende il medesimo valore, per il teorema testè citato essa è una funzione razionale di t. Le sostituzioni del gruppo di monodromia Γ debbono dunque lasciarla invariata ed appartengono per ciò a Λ c. d. d.

È chiaro poi che mentre la definizione primitiva del gruppo Λ era relativa ad un punto A (non critico) fissato nel piano, risulta ora che questo gruppo Λ non varia cangiando comunque il punto A di partenza, ciò che del resto è facile a vedersi direttamente.

§. 110. — Per illustrare le teorie generali svolte nei §§. precedenti, consideriamo le equazioni per la divisione dell'argomento nelle funzioni circolari, p. e. quella che, essendo data

$$t = \cos w,$$

fa conoscere

$$x = \cos\left(\frac{w}{m}\right),$$

indicando m un numero intero e dimostriamone la risolubilità per radicali. Poichè per $m = 2$ si ha la ben nota formola

$$x = \pm\sqrt{\frac{1+t}{2}},$$

basterà limitarsi al caso in cui il divisore m sia un numero primo

dispari p, potendosi manifestamente risalire da questo caso particolare al caso generale. Dalla formola di MOIVRE

$$\left(\cos\frac{w}{p} + i \operatorname{sen}\frac{w}{p}\right)^p = \cos w + i \operatorname{sen} w$$

segue che x è legata a t dall'equazione di grado $= p$:

$$(a) \quad x^p - \frac{p\,(p-1)}{1\,.\,2}\,x^{p-2}(1-x^2) + \frac{p\,(p-1)(p-2)(p-3)}{1\,.\,2\,.\,3\,.\,4}\,x^{p-4}(1-x^2)^2 + \ldots = t$$

e le sue p radici sono

$$x_0 = \cos\frac{w}{p}\,,\quad x_1 = \cos\frac{w+2\pi}{p}\,,\ \ldots\ x_{p-1} = \cos\frac{w+2\,(p-1)\,\pi}{p}\,.$$

Il gruppo Γ di monodromia si determina facilmente, osservando che, se $t = \cos w$ deve descrivere nel suo piano complesso un cammino chiuso, bisogna che w si cangi in $\pm\, w + 2\,\beta\,\pi$, con β intero, e viceversa, qualunque sia β, se w varia con continuità da w a $\pm\, w + 2\,\beta\,\pi$, la t descrive nel suo piano complesso un cammino chiuso. Ogni ramo x_ν della nostra funzione algebrica si cangia, per questa sostituzione, nel ramo $x_{\nu'}$, il cui indice ν' è definito dalla congruenza

$$(b) \qquad \nu' \equiv \pm\,\nu + \beta \pmod{p}.$$

Le $2p$ sostituzioni (b), ove si diano a β tutti i suoi valori, costituiscono quindi il gruppo di monodromia Γ della nostra equazione (a).

È facile poi vedere che se al campo assoluto di razionalità si aggiunge l'irrazionale numerico $\cos\frac{2\pi}{p}$, il gruppo algebrico dell'equazione coinciderà precisamente con Γ. Intanto il gruppo algebrico, dovendo contenere il gruppo di monodromia (b) come sottogruppo invariante, non potrà contenere alcuna sostituzione fuori del gruppo metaciclico (§. 35). Sia ora $\nu' \equiv a\,\nu + b \pmod{p}$ una sostituzione del detto gruppo algebrico, dopo l'aggiunta di $\cos\frac{2\pi}{p}$. Abbiamo

$$\cos\frac{w+2\pi}{p} + \cos\frac{w-2\pi}{p} = 2\cos\frac{2\pi}{p}\cos\frac{w}{p}\,,$$

cioè

$$(c) \qquad x_1 + x_{-1} - 2 \cos \frac{2\pi}{p} . x_0 = 0$$

e a questa relazione sarà applicabile qualunque sostituzione dell'attuale gruppo di Galois p. e. la $\nu' \equiv a\nu$ che dà

$$x_a + x_{-a} - 2 \cos \frac{2\pi}{p} . x_0 = 0.$$

D'altra parte si ha

$$x_a + x_{-a} = \cos \frac{w + 2a\pi}{p} + \cos \frac{w - 2a\pi}{p} = 2 \cos a . \frac{2\pi}{p} . x_0$$

e si conclude quindi $a \equiv \pm 1 \pmod{p}$ c. d. d.

Si osservi poi che l'aggiunta dell'irrazionale numerico $\cos \frac{2\pi}{p}$ è certamente necessaria, se si vuole abbassare il gruppo algebrico G dell'equazione nel campo assoluto di razionalità al gruppo di monodromia Γ, poichè la funzione razionale delle radici della (a)

$$\frac{x_1 + x_{-1}}{2 x_0} = \cos \frac{2\pi}{p}$$

è invariabile per tutte le sostituzioni (b) di Γ. Dopo ciò è ben facile determinare il gruppo algebrico della (a) nel campo assoluto di razionalità. Questo gruppo G non può essere infatti che il gruppo metaciclico, od un suo sottogruppo d'ordine multiplo di $2p$. Ma il secondo caso si esclude perchè allora l'indice di Γ in G sarebbe un divisore puro di $\frac{p-1}{2}$ e siccome il gruppo $\frac{G}{\Gamma}$ è un gruppo Abeliano ciclico, basterebbe la risoluzione della corrispondente equazione Abeliana d'ordine $< \frac{p-1}{2}$ per far conoscere razionalmente $2 \cos \frac{2\pi}{p} = e^{\frac{2\pi i}{p}} + e^{\frac{-2\pi i}{p}} = \varepsilon + \varepsilon^{-1}$, che dipende, come sappiamo, da un'equazione Abeliana irriducibile di grado $= \frac{p-1}{2}$. Dunque: *Il gruppo algebrico dell'equazione (a) per la divisione dell'argomento per p della funzione circolare cos w, nel campo assoluto di razionalità, è il gruppo metaciclico $\nu' \equiv a\nu + b \pmod{p}$, che si riduce al gruppo*

di monodromia $\nu' \equiv \pm \nu + b \pmod{p}$ *coll'aggiunta dell'irrazionale numerico* $\cos \frac{2\pi}{p}$.

Se ne ricava in particolare che queste equazioni per la divisione dell'argomento nelle funzioni circolari sono sempre risolubili per radicali. Ma si osservi che, già nel caso $p = 3$, è *necessaria* l'estrazione di un radicale d'indice superiore a 2, qui di un radicale cubico, e perciò il corrispondente problema geometrico (trisezione dell'angolo) non è solubile *in generale* colla riga e col compasso.

§. 111. — Ci volgiamo ora alle ultime ricerche che ci proponiamo di esporre nel presente libro, trattando di quelle funzioni algebriche i cui rami sono tutti funzioni lineari (fratte), a coefficienti costanti, di uno dei rami stessi. Le corrispondenti equazioni (dei poliedri regolari) hanno importanza fondamentale in molte teorie d'analisi. Il primo e più semplice esempio di equazioni di questa specie è fornito dall'equazione ciclica

$$x^m = t,$$

ove appunto tutti i rami si esprimono linearmente per uno di essi x_0 colla formola

$$x_r = \varepsilon^r x_0 \begin{cases} \varepsilon = e^{\frac{2\pi i}{m}} \\ r = 0, 1, 2, \ldots m-1. \end{cases}$$

Andiamo subito a dimostrare come il problema di costruire tutte le equazioni irriducibili ad un parametro, dotate della proprietà voluta, si riconduca ad un problema già risoluto nella prima parte di questo libro e cioè alla determinazione dei gruppi finiti di sostituzioni lineari sopra una variabile x. (Cap. IV). Sia

$$f(x, t) = 0 \tag{5}$$

un'equazione irriducibile di grado m in x, tale che indicando con x un ramo (una delle radici della (5)), tutti gli altri rami siano funzioni lineari di x, che indicheremo con

$$\frac{a_i x + b_i}{c_i x + d_i} \qquad (i = 1, 2, \ldots m-1),$$

i coefficienti a, b, c, d essendo costanti assolute.

Se conveniamo di fare

$$a_0 = d_0 = 1 \ , \ b_0 = c_0 = 0 \, ,$$

potremo dire che tutti gli m rami della funzione algebrica $x(t)$ sono contenuti nella formola

$$\frac{a_i x + b_i}{c_i x + d_i} \qquad (i = 0, 1, 2 \ldots m-1) \, . \tag{6}$$

Dimostriamo ora: *Le m sostituzioni lineari* (6) *sulla variabile x formano un gruppo.*

Servendoci di considerazioni della teoria delle funzioni, stabiliamo subito il teorema osservando che se

$$x' = \frac{a_i x + b_i}{c_i x + d_i} \ , \ x'' = \frac{a_k x + b_k}{c_k x + d_k}$$

sono due qualunque dei rami, esisterà, a causa dell'irriducibilità dell'equazione (ossia della transitività del gruppo di monodromia), un cammino chiuso che porterà il ramo x in x', cioè x in $\frac{a_i x + b_i}{c_i x + d_i}$ e il medesimo cammino chiuso cangierà quindi con continuità $x'' = \frac{a_k x + b_k}{c_k x + d_k}$ in

$$\frac{a_k \dfrac{a_i x + b_i}{c_i x + d_i} + b_k}{c_k \dfrac{a_i x + b_i}{c_i x + d_i} + d_k} \, ,$$

che sarà per ciò un altro ramo della funzione.

Dunque la sostituzione composta

$$\begin{pmatrix} a_i \, , & b_i \\ c_i \, , & d_i \end{pmatrix} \cdot \begin{pmatrix} a_k \, , & b_k \\ c_k \, , & d_k \end{pmatrix}$$

appartiene ancora alle (6) c. d. d.

Si arriva alla medesima conclusione per via algebrica, osservando che l'equazione

$$f\left(\frac{a_k x + b_k}{c_k x + d_k}, t\right) = 0$$

ha colla equazione irriducibile (5) la radice x a comune e per ciò le ammette tutte, in particolare $\frac{a_i x + b_i}{c_i x + d_i}$.

Così vediamo che ad ogni equazione (5), dotata della voluta proprietà, corrisponde un gruppo finito (6) di sostituzioni lineari sopra una variabile.

È chiaro poi che qualunque sostituzione $\begin{pmatrix} a_i\,, & b_i \\ c_i\,, & d_i \end{pmatrix}$ del gruppo, applicata ad un ramo *qualsiasi* della nostra funzione algebrica, dà sempre un altro ramo.

§. 112. — Dimostriamo inversamente che per ogni gruppo (6) di sostituzioni lineari si può costruire una corrispondente equazione (5), i cui rami sono appunto legati l'uno all'altro da una sostituzione del gruppo. Per questo basta costruire, come subito vedremo, una funzione razionale della x che non cangi di valore applicando all'argomento x una sostituzione qualunque del gruppo [1]). A tale oggetto prendiamo due costanti arbitrarie A, B, che soltanto assoggettiamo alla condizione di non essere fra loro *equivalenti* rispetto al gruppo (6), cioè supponiamo che *non* si abbia per alcun valore dell'indice i:

$$B = \frac{a_i A + b_i}{c_i A + d_i} \qquad (i = 0, 1, 2, \ldots m-1)\ ,$$

e costruiamo la funzione razionale

$$(7) \qquad F(x) = \frac{\prod\limits_{i=0}^{i=m-1} \left(\dfrac{a_i x + b_i}{c_i x + d_i} - A \right)}{\prod\limits_{i=0}^{i=1} \left(\dfrac{a_i x + b_i}{c_i x + d_i} - B \right)}\ ,$$

che sarà la funzione richiesta. E infatti qualunque sostituzione del gruppo (6), eseguita sull'argomento x, non fa che scambiare fra loro i fattori al numeratore e al denominatore della (7). La (7) può scriversi

$$(7^*) \qquad F(x) = \frac{\varphi(x)}{\psi(x)}\ ,$$

---

[1]) Le funzioni qui considerate sono le prime e più semplici della classe delle funzioni *automorfe* (Kleiniane e Fuchsiane secondo POINCARÉ), che si riproducono per un gruppo finito o infinito di sostituzioni lineari sull'argomento.

essendo $\varphi(x)$, $\psi(x)$ polinomii razionali interi di grado m in x, definiti dalle formole:

$$(8)\qquad \begin{cases} \varphi(x) = \prod\limits_{i=0}^{i=m-1} \left\{ (a_i x + b_i) - \mathrm{A}(c_i x + d_i) \right\} \\ \psi(x) = \prod\limits_{i=0}^{i=m-1} \left\{ (a_i x + b_i) - \mathrm{B}(c_i x + d_i) \right\} \end{cases} .$$

Si osservi che le radici di $\varphi(x) = 0$ sono gli m valori di x equivalenti ad A e similmente le radici di $\psi(x) = 0$ sono gli m valori equivalenti a B, onde, per le ipotesi fatte, *i due polinomii* $\varphi(x)$, $\psi(x)$ *risultano primi fra loro.*

Indicando con t un parametro, si consideri l'equazione

$$\mathrm{F}(x) = \frac{\varphi(x)}{\psi(x)} = t\,;$$

gli m rami della funzione algebrica x di t, così definita dall'equazione *irriducibile* [1]) di grado m

$$(9)\qquad \varphi(x) - t\,\psi(x) = 0,$$

saranno appunto legati ad uno qualunque di essi dalle sostituzioni lineari del gruppo dato (6).

Corrispondentemente ai cinque tipi di gruppi di sostituzioni lineari (Cap. IV), avremo cinque tipi di equazioni (9). Queste diconsi le *equazioni dei poliedri regolari*, a causa della rappresentazione geometrica del gruppo come gruppo di rotazioni dei poliedri regolari. (Cap. IV).

§. 113. — È facile determinare il gruppo di monodromia delle equazioni (9) dei poliedri regolari. Per ciò si osservi che, indicando con

$$(10)\qquad x_0,\ x_1,\ x_2 \ldots x_{m-1}$$

gli m rami della funzione algebrica, si avrà

$$x_i = \frac{a_i x_0 + b_i}{c_i x_0 + d_i} \quad (i = 0,\ 1,\ 2 \ldots m-1)\,.$$

---

[1]) Che la (9) sia irriducibile risulta subito dal fatto che il parametro t vi entra linearmente, mentre $\varphi(x)$, $\psi(x)$ sono primi fra loro. Se $\varphi(x) - t\,\psi(x)$ si scindesse in due fattori, l'uno di essi sarebbe indipendente da t e sarebbe fattor comune di $\varphi(x)$, $\psi(x)$.

Se in questa formola cangiamo x_0 in un altro qualunque x_k dei rami, le nuove espressioni

$$\bar{x}_i = \frac{a_i x_k + b_i}{c_i x_k + b_i} \quad (i = 0, 1, 2 \ldots m-1)$$

saranno gli m rami (10) in altro ordine. Ad ogni sostituzione $\begin{pmatrix} a_k, b_k \\ c_k, d_k \end{pmatrix}$ del gruppo corrisponde così una determinata sostituzione γ_k sugli m rami (10) e le m sostituzioni

$$\gamma_0, \gamma_1 \ldots \gamma_{m-1}$$

corrispondenti formano un gruppo Γ di sostituzioni oloedricamente isomorfo al gruppo fondamentale (6) di sostituzioni lineari. Ora dimostriamo: *Questo gruppo Γ è il gruppo di monodromia dell'equazione.*

E infatti il gruppo di monodromia è certamente transitivo e siccome per una qualunque delle radici x_i della proposta tutte le altre si esprimono razionalmente (linearmente) vi è in Γ una ed una sola sostituzione che porta x_0 in x_k. Nella relazione

$$x_i = \frac{a_i x_0 + b_i}{c_i x_0 + d_i}$$

eseguendo questa sostituzione di Γ, si vede appunto che x_i si cangia in

$$\bar{x}_i = \frac{a_i x_k + b_i}{c_i x_k + d_i} \text{ [1]}.$$

Possiamo di più domandare in quale campo di razionalità il gruppo algebrico dell'equazione coinciderà col gruppo di monodromia Γ. Basterà per ciò ampliare il campo di razionalità dei coefficienti della proposta (9) coll'aggiunta degli irrazionali numerici che eventualmente figurassero nei coefficienti $\begin{pmatrix} a_i, b_i \\ c_i, d_i \end{pmatrix}$ del gruppo, senza comparire nei coefficienti della (9) sviluppata.

Dobbiamo dimostrare che, dopo tale aggiunta, una funzione razionale

$$F(x_0, x_1 \ldots x_{m-1}, t)$$

---

[1]) La medesima cosa risulta da considerazioni di continuità, poichè un cammino chiuso che cangi x_0 in x_k cangerà pure con continuità $\frac{a_i x_0 + b_i}{c_i x_0 + d_i}$ in $\frac{a_i x_k + b_i}{c_i x_k + d_i}$.

degli m rami e di t che rimanga invariata per le sostituzioni di Γ sarà razionalmente nota. E infatti, esprimendo $x_1, x_2 \ldots x_m$ per x_0, avremo

$$F(x_0, x_1, x_2, \ldots x_{m-1}, t) = \psi(x_0, t),$$

dove $\psi(x_0, t)$ è razionale in x_0, t, con coefficienti appartenenti al campo ampliato. La funzione razionale delle x e di t

$$F(x_0 x_1 \ldots x_{m-1}, t) - \psi(x_0, t)$$

è razionalmente nota per t, essendo $= 0$, e deve quindi rimanere invariata per tutte le sostituzioni di Γ. Se ne trae

$$\psi(x_0, t) = \psi(x_1, t) = \ldots = \psi(x_{m-1}, t),$$

onde segue che

$$F(x_0, x_1, \ldots x_{m-1}, t) = \frac{1}{m}\left\{\psi(x_0, t) + \psi(x_1, t) + \ldots + \psi(x_{m-1}, t)\right\},$$

come funzione simmetrica di $x_0, x_i \ldots x_{m-1}$, è razionale in t c. d. d.

In fine possiamo vedere quali e quanti saranno nel piano complesso t i punti critici della nostra equazione (9). Se $t = t_0$ è un tale punto critico, ove p. e. coincidano con x_0 i ν rami

$$x_0 x_1 \ldots x_{\nu-1},$$

tutti gli m rami coincideranno, in $t = t_0$, ν a ν poichè, essendo $\begin{pmatrix} a, b \\ c, d \end{pmatrix}$ una sostituzione qualunque del gruppo, i ν rami

$$\frac{a x_0 + b}{c x_0 + d}, \frac{a x_1 + b}{c x_1 + d}, \ldots \frac{a x_{\nu-1} + b}{c x_{\nu-1} + d}$$

coincidono in $t = t_0$ nè possono coincidervi in numero maggiore, chè se fosse $\dfrac{a x_\nu + b}{c x_\nu + d} = \dfrac{a x_0 + b}{c x_0 + d}$ ne verrebbe $x_\nu = x_0$. Il valor comune

$$x_0 = x_1 = x = \ldots = x_{\nu-1}$$

è evidentemente, secondo le denominazioni dei §§. 43, 44, un polo comune precisamente a ν sostituzioni del gruppo e cioè

$$\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}, \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \ldots \begin{pmatrix} a_{\nu-1} & b_{\nu-1} \\ c_{\nu-1} & d_{\nu-1} \end{pmatrix}$$

e viceversa ogni polo $x = \xi$, comune a ν sostituzioni del gruppo, è il

valor comune di ν rami coincidenti per la nostra funzione algebrica. Gli $\frac{m}{\nu}$ valori distinti dei rami in $t = t_0$ sono quindi un sistema completo di poli fra loro equivalenti, onde risulta che sono tanti i punti critici della nostra equazione quante classi di poli non equivalenti hanno le sostituzioni del gruppo e però, secondo la classificazione dei tipi del Cap. IV, avremo in ogni caso *tre punti critici* salvo per le equazioni appartenenti al tipo I) (equazioni cicliche), ove il numero dei poli sarà di due soltanto.

§. 114. — Le equazioni dei poliedri regolari appartenenti ai primi quattro tipi e cioè le equazioni della piramide o della doppia piramide regolare e quelle del tetraedro e dell'ottaedro hanno gruppi risolubili; queste equazioni sono quindi risolubili per radicali, cioè riducibili a successive equazioni binomie. Non così l'equazione dell'icosaedro, il cui gruppo è semplice. L'irrazionalità semplice da essa definita (irrazionalità dell'icosaedro) è quindi di natura diversa da quelle definite per estrazioni di radicali. Se oltre all'aggiunta di radicali permettiamo quella di questa nuova irrazionalità, viene naturalmente ad ampliarsi il campo delle equazioni risolubili ed in questo senso appunto, come vedremo, l'equazione generale di 5.° grado diventa risolubile per irrazionalità icosaedrica e per radicali. Lasciando da parte lo studio delle altre irrazionalità dei poliedri regolari, ci proponiamo ora di studiare l'equazione dell'icosaedro e le sue più importanti risolventi per far conoscere i principii della teoria di Klein dal cui libro [1]) togliamo appunto, salvo modificazioni di secondaria importanza, le ricerche dei §§. seguenti.

I calcoli che dovremo eseguire verranno molto facilitati dall'uso delle variabili omogenee e dei primi teoremi della teoria delle forme algebriche. In primo luogo andiamo a scrivere sotto forma omogenea le sostituzioni del gruppo icosaedrale.

Osserviamo dapprima che se nella formola di Cayley (I) §. 51:

$$(11) \qquad z' = \frac{A z + B}{-B_0 z + A_0}, \quad A A_0 + B B_0 = 1,$$

---

[1]) *Vorlesungen über das Ikosader und die Auflösung der Gleichungen von fünften Grade.* (Leipzig-Teubner 1884).

cangiamo la variabile z nel quoziente di due nuove variabili $\frac{z_1}{z_2}$ e similmente la trasformata z' in $\frac{z'_1}{z'_2}$, alla sostituzione non omogenea (11), possiamo coordinare l'altra omogenea

$$(12) \qquad \begin{cases} \pm z'_1 = A\, z_1 + B\, z_2 \\ \pm z'_2 = -B_0 z_1 + A_0 z_2 , \end{cases}$$

nella quale, fissando che il determinante della sostituzione debba essere l'unità, resterà ancora la scelta fra le due determinazioni di segno. Per ciò ad ogni sostituzione non omogenea (11) ne corrisponderanno due omogenee (12), ad una di queste una sola di quelle. Se consideriamo un gruppo G_N di N sostituzioni non omogenee (11), avremo corrispondentemente un gruppo G_{2N} di 2N sostituzioni omogenee (12), che sarà evidentemente isomorfo, col grado 2 di meriedria, con G_N, all'identità in G_N corrispondendo in G_{2N} il sottogruppo invariante di 2.° ordine formato dalle due sostituzioni

$$z'_1 = \pm z_1 \quad , \quad z'_2 = \pm z_2 .$$

Qui si presenta naturalmente la domanda [1]:

È possibile fra le due determinazioni di segno nella (12) *sceglierne ogni volta una in guisa da ottenere un gruppo omogeneo di* N *sostituzioni oloedricamente isomorfo con* G_N?

Pel nostro scopo ci basta osservare che una tal cosa è già impossibile per un gruppo diedrale di 4 sostituzioni (Vierergruppe). E infatti, secondo le ricerche del §. 46, possiamo dare alle quattro sostituzioni corrispondenti la forma normale

$$z' = \pm z \quad , \quad z' = \pm \frac{1}{z}$$

e le corrispondenti 8 sostituzioni omogenee sono

$$\begin{pmatrix} \pm 1 , & 0 \\ 0 , & \pm 1 \end{pmatrix} , \begin{pmatrix} \pm i , & 0 \\ 0 , & \mp i \end{pmatrix} , \begin{pmatrix} 0 , & \pm i \\ \pm i , & 0 \end{pmatrix} , \begin{pmatrix} 0 , & \pm 1 \\ \mp 1 , & 0 \end{pmatrix} .$$

---

[1]) Klein *l. c.*, p. 45.

Ora nel gruppo omogeneo figura necessariamente l'identità $\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$, sicchè basta mostrare che vi figura anche l'altra $\begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix}$ per rendere evidente che la detta scelta di segni è impossibile. Ciò risulta subito dall'osservare che l'una e l'altra sostituzione $\begin{pmatrix} i, & 0 \\ 0, & -i \end{pmatrix}$, $\begin{pmatrix} -i, & 0 \\ 0, & i \end{pmatrix}$ elevate al quadrato danno appunto $\begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix}$.

Ora il gruppo dell'icosaedro, come pure quelli del tetraedro e dell'ottaedro, contengono sottogruppi diedrali di 4 sostituzioni e però anche qui la cosa domandata è impossibile.

Vogliamo ora scrivere le sostituzioni omogenee del gruppo icosaedrale, per la qual cosa basterà riferirsi alla forma normale che nel §. 49 abbiamo dato alle sostituzioni di questo gruppo e in particolare ricordare che esso si genera colle due sostituzioni elementari

$$\text{S)} \quad z' = \varepsilon z$$

$$\text{T)} \quad z' = \frac{(\varepsilon^4 - \varepsilon) z + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3) z - (\varepsilon^4 - \varepsilon)} \qquad \left(\varepsilon = e^{\frac{2\pi i}{5}}\right).$$

Riducendo le corrispondenti sostituzioni omogenee al determinante 1, avremo:

$$(13) \qquad \text{per la S} \begin{cases} z'_1 = \pm \varepsilon^3 z_1 \\ z'_2 = \pm \varepsilon^2 z_2 \end{cases}$$

$$(13^*) \qquad \text{per la T} \begin{cases} \sqrt{5} \,.\, z'_1 = \pm \{(\varepsilon^4 - \varepsilon) z_1 + (\varepsilon^2 - \varepsilon^3) z_2\} \\ \sqrt{5} \,.\, z'_2 = \pm \{(\varepsilon^2 - \varepsilon^3) z_1 - (\varepsilon^4 - \varepsilon) z_2\} \end{cases}$$

e con queste due sostituzioni genereremo l'intero gruppo omogeneo icosaedrale G_{120}. È bene osservare che siccome questo G_{120} è isomorfo col gruppo icosaedrale G_{60} e questo è semplice, così: *Il gruppo omogeneo icosaedrale* G_{120} *non ha altro sottogruppo invariante che il gruppo del 2.° ordine*

$$z'_1 = \pm z_1 \quad , \quad z'_2 = \pm z_2 \,.$$

§. 115. — Introduciamo ora la nozione di forme invarianti del gruppo omogeneo icosaedrale G_{120} colla definizione seguente:

Una forma binaria $\Phi(z_1, z_2)$ *si dirà un invariante del gruppo icosaedrale omogeneo* G_{120}, *quando per ogni sostituzione di questo gruppo essa si riproduca, moltiplicata per un fattore costante.*

Eguagliando a zero una tale forma

$$\Phi(z_1, z_2) = 0,$$

i valori radici $z = \frac{z_1}{z_2}$ avranno per indici sulla sfera complessa un sistema di punti, che per tutte le 60 rotazioni del gruppo dell'icosaedro si scambieranno fra loro.

Viceversa se si ha sulla sfera un tale sistema di m punti, che supponiamo distinti, e si costruisce la funzione $F(z)$ che li ha per indici delle sue radici, indi, mutato z in $\frac{z_1}{z_2}$, si moltiplica $F\left(\frac{z_1}{z_2}\right)$ per z_2^m, cangeremo $F\left(\frac{z_1}{z_2}\right)$ in una forma $\Phi(z_1, z_2)$ che sarà evidentemente un invariante icosaedrale. È da osservarsi che, ove fra i punti del sistema figurasse il polo $z = \infty$, ciò sarebbe semplicemente caratterizzato nella forma invariantiva $\Phi(z_1, z_2)$ dal presentarsi del fattore z_2.

Se il sistema di punti radici della forma invariante $\Phi(z_1, z_2)$ si scinde in più sistemi di punti equivalenti rispetto al gruppo delle 60 rotazioni, corrispondentemente la forma $\Phi(z_1, z_2)$ si scinderà nel prodotto di altrettante forme parziali che diremo *forme fondamentali*. In generale una forma fondamentale dell'icosaedro sarà di grado $= 60$ perchè un suo punto radice, occupa, per le 60 rotazioni dell'icosaedro, 60 posizioni in generale distinte. Fanno eccezione soltanto i 12 vertici dell'icosaedro, i 20 punti medii delle faccie (proiettati dal centro sulla sfera) e in fine i 30 punti medii delle costole, cioè insomma i vertici delle tre specie nella rete icosaedrica (§. 57). Corrispondentemente avremo tre forme fondamentali dei gradi 12, 20 e 30, che indicheremo rispettivamente con

$$f, \quad H, \quad T.$$

Se indichiamo quindi con N il grado di una forma invariante qualsiasi, dovremo avere

$$(a) \qquad N = \alpha \,.\, 60 + \beta \,.\, 12 + \gamma \,.\, 20 + \delta \,.\, 30,$$

essendo $\alpha, \beta, \gamma, \delta$ numeri interi positivi o nulli.

È facile ora vedere *a priori*, pel modo di composizione del gruppo G_{120}, che le forme fondamentali f, H, T e qualunque altra forma invariantiva $\Phi(z_1, z_2)$ si riproducono assolutamente per qualunque sostituzione del gruppo omogeneo icosaedrale [1]). Supponiamo infatti che la forma invariante $\Phi(z_1, z_2)$ acquisti, per le diverse sostituzioni di G_{120}, i fattori differenti

$$(14) \qquad a_1, \; a_2 \ldots a_\nu .$$

Se per due sostituzioni g, g' di G_{120} la Φ acquista i rispettivi fattori a, a', per la sostituzione composta gg' acquista il fattore prodotto dei due aa', onde i ν numeri (14) debbono formare un gruppo, cioè il prodotto di due qualunque numeri (14) è di nuovo uno di essi. Questo gruppo essendo d'ordine $= \nu$, si ha quindi per ciascuno dei numeri (14) $a^\nu = 1$ e, siccome sono ν differenti, vediamo che posto $\varepsilon = e^{\frac{2\pi i}{\nu}}$ i moltiplicatori (14) saranno dati, in altro ordine, dalle potenze di ε

$$1, \varepsilon, \varepsilon^2 \ldots \varepsilon^{\nu-1} .$$

Prendiamo una sostituzione g di G_{120} che operata sulla Φ produca in questa la moltiplicazione per ε; sia poi A la rotazione del gruppo dell'icosaedro corrispondente a g ed r il suo periodo. Ad $A^r = 1$ corrisponderà nel gruppo omogeneo la g^r, che sarà l'una o l'altra delle due sostituzioni $z'_1 = \pm z_1$, $z'_2 = \pm z_2$, le quali lasciano certamente Φ inalterata perchè, a causa della (a), *ogni formazione invariante dell'icosaedro è di grado pari.*

Se ne conclude $\varepsilon^r = 1$ e poichè le rotazioni del gruppo icosaedrale non offrono che i periodi $r = 2, 3, 5$ ne seguirà intanto

$$\nu = 1, \text{ o } \nu = 2 \text{ o } \nu = 3, \text{ o } \nu = 5.$$

D'altra parte quelle sostituzioni di G_{120}, cui corrisponde il moltiplicatore 1 per la $\Phi(z_1, z_2)$, formano evidentemente in G_{120} un sottogruppo invariante d'indice ν sicchè, per l'osservazione in fine al §. precedente, si avrà

$$\nu = 1 \text{ o } \nu = 60 \text{ o } \nu = 120$$

---

[1]) La costruzione effettiva dalle forme f, H, T (§. seguente) confermerà la proprietà.

Abbiamo quindi necessariamente $\nu = 1$, il che dimostra la proprietà enunciata.

Se consideriamo le potenze

$$f^5,\ H^3,\ T^2,$$

avremo tre forme invarianti di grado 60 e con due qualunque di esse potremo comporre linearmente ed omogeneamente, con coefficienti costanti, qualsiasi forma fondamentale $\Phi(z_1, z_2)$, cioè sussisterà p. e. la relazione

$$\Phi(z_1, z_2) = \lambda . f^5 + \mu . H^3, \tag{15}$$

con λ, μ costanti. Per dimostrarlo basta osservare che una forma fondamentale è già determinata, a meno di un fattore costante, quando sia fissata una delle sue radici. Ora il secondo membro della (15) è sempre manifestamente una forma invariante e, dando al rapporto $\frac{\lambda}{\mu}$ un conveniente valore, possiamo dare ad una delle sue radici qualunque valore.

In particolare risulta di qui il teorema:

Fra le tre potenze f^5, H^3, T^2 sussiste una relazione lineare omogenea a coefficienti costanti.

§. 116. — Cominciamo dal costruire la forma f, i cui punti radici sono nei 12 vertici dell'icosaedro, cioè nei punti (Cap. IV §. 56):

$$z = 0,\ \infty,\ \varepsilon^r(\varepsilon+\varepsilon^4),\ \varepsilon^r(\varepsilon^2+\varepsilon^3)\ (r = 0, 1, 2, 3, 4).$$

Possiamo quindi porre

$$f = z_1 z_2 \prod_{r=0}^{r=4} \{ z_1 - \varepsilon^r(\varepsilon+\varepsilon^4) z_2 \} . \{ z_1 - \varepsilon^r(\varepsilon^2+\varepsilon^3) z_2 \}$$

e poichè si ha in generale

$$\prod_{r=0}^{r=4} (z_1 - \varepsilon^r z_2) = z_1^5 - z_2^5,$$

sarà

$$f = z_1 z_2 [z_1^5 - (\varepsilon+\varepsilon^4)^5 z_2^5] . [z_1^5 - (\varepsilon^2+\varepsilon^3)^5 z_2^5].$$

Ma, avendosi

$$(\varepsilon + \varepsilon^4)\,(\varepsilon^2 + \varepsilon^3) = -1$$

$$(\varepsilon + \varepsilon^4)^5 + (\varepsilon^2 + \varepsilon^3)^5 = -11\,,$$

troveremo

$$f = z_1\, z_2\, (z_1^{10} + 11\, z_1^5\, z_2^5 - z_2^{10}) \tag{16}$$

Per calcolare H e T potremmo procedere similmente, servendoci dei valori di z nei loro punti radici, ciò che otterremmo cercando i poli delle rispettive rotazioni coi periodi 3 e 2. In modo più breve ed elegante perveniamo allo scopo osservando che la *forma Hessiana* della f, cioè il determinante

$$\begin{vmatrix} \dfrac{\partial^2 f}{\partial z_1^2} & \dfrac{\partial^2 f}{\partial z_1\, \partial z_2} \\[2ex] \dfrac{\partial^2 f}{\partial z_2\, \partial z_1} & \dfrac{\partial^2 f}{\partial z_2^2} \end{vmatrix}$$

è appunto di grado 20 ed essendo un covariante di f essa rimane, come f, totalmente invariata per ogni sostituzione omogenea del gruppo icosaedrale. Ora nella formola (a) del §. precedente, avendosi qui $N = 20$, sarà necessariamente

$$\alpha = \beta = \delta = 0\,,\ \gamma = 1\,,$$

cioè: *L'Hessiana di f coincide, a meno di un fattore numerico, colla forma* H:

Poniamo con Klein:

$$H = \frac{1}{11^2} \begin{vmatrix} \dfrac{\partial^2 f}{\partial z_1^2}\,, & \dfrac{\partial^2 f}{\partial z_1\, \partial z_2} \\[2ex] \dfrac{\partial^2 f}{\partial z_2\, \partial z_1}\,, & \dfrac{\partial^2 f}{\partial z_2^2} \end{vmatrix}$$

e col calcolo effettivo troviamo

$$H = -(z_1^{20} + z_2^{20}) + 228\,(z_1^{15}\, z_2^5 - z_1^5\, z_2^{15}) - 494\, z_1^{10}\, z_2^{10}. \tag{17}$$

Similmente è un covariante di f la forma Jacobiana di f e di H:

$$\begin{vmatrix} \frac{\partial f}{\partial z_1} & \frac{\partial f}{\partial z_2} \\ \frac{\partial H}{\partial z_1} & \frac{\partial H}{\partial z_2} \end{vmatrix},$$

che è quindi una forma invariante icosaedrale di grado $= 30$ e coincide per ciò, salvo un fattore numerico, con T. Disponendo di questo fattore numerico, poniamo:

$$T = -\frac{1}{20} \begin{vmatrix} \frac{\partial f}{\partial z_1}, & \frac{\partial f}{\partial z_2} \\ \frac{\partial H}{\partial z_1}, & \frac{\partial H}{\partial z_2} \end{vmatrix}$$

e troveremo collo sviluppo effettivo

$$(18) \qquad T = z_1^{30} + z_2^{30} + 522\,(z_1^{25}\, z_2^5 - z_1^5\, z_2^{25}) - 10005\,(z_1^{20}\, z_2^{10} + z_1^{10}\, z_2^{20}).$$

Come già abbiamo sopra osservato, il quadrato della forma T è una combinazione lineare omogenea di f^5, H^3:

$$T^2 = \lambda f^5 + \mu\, H^3$$

e basta confrontare dall'una parte e dall'altra i coefficienti dei termini in $z_1^{60}\, z_1^{55}\, z_2^5$ per trovare

$$\lambda = 1728 = 12^3,\ \mu = -1;$$

la relazione fra f^5, H^3, T^2 è dunque

$$(19) \qquad T^2 + H^3 = 1728\, f^5 = 12^3\, f^5$$

§. 117. — I risultati superiori e le osservazioni generali al §. 112 per la costruzione delle equazioni dei poliedri regolari ci pongono in grado di scrivere l'equazione dell'icosaedro, eguagliando il quoziente di due forme fondamentali di grado 60 al parametro, che indicheremo ora con Z, e ponendo poi $z = \frac{z_1}{z_2}$. Da quanto abbiamo detto alla fine del §. 115, risulta che l'arbitrarietà che resta nella costruzione

dell'equazione dell'icosaedro corrisponde a far subire al parametro Z una sostituzione lineare fratta. Fissiamo con KLEIN l'equazione dell'icosaedro ponendo

$$\text{(I)} \qquad \frac{H^3}{12^3 f^5} = Z$$

e, per l'identità (19), potremo anche scrivere l'equazione dell'icosaedro sotto forma di proporzione continua:

$$\text{(I*)} \qquad Z : Z-1 : 1 = H^3 : -T^2 : 12^3 f^5 .$$

L'equazione del 60.° grado dell'icosaedro, scritta per disteso, sarà dunque:

$$\text{(II)} \quad (z^{20} - 228 z^{15} + 494 z^{10} + 228 z^5 + 1)^3 - 12^3 z^5 (z^{10} + 11 z^5 - 1)^5 . Z = 0 .$$

Essa ha, come si vede, coefficienti razionali e interi e definisce la funzione algebrica z di Z, i cui 60 rami si ottengono l'uno dall'altro colle 60 sostituzioni del gruppo icosaedrale. I tre punti critici dell'equazione (II) dell'icosaedro nel piano Z sono rispettivamente

$$Z = 0 , Z = 1, Z = \infty ,$$

ai quali corrispondono per la z valori che hanno rispettivamente per indici i punti medii delle facce, i punti medii delle costole ed in fine i vertici stessi dell'icosaedro, come risulta dalla (I*). La nostra rappresentazione geometrica, mediante la rete icosaedrale, rende evidente che, girando attorno a $Z = 0$, i 60 rami dell'irrazionalità icosaedrica subiscono una sostituzione ciclica del 3.° ordine (si permutano 3 a 3), similmente attorno a $Z = 1$ si permutano 2 a 2 e intorno a $Z = \infty$ 5 a 5.

Sappiamo già (§. 113) che il gruppo Γ di monodromia dell'equazione dell'icosaedro è precisamente d'ordine 60 ed oloedricamente isomorfo col gruppo di rotazioni icosaedrale. L'irrazionalità numerica, la cui aggiunta abbassa il gruppo algebrico G al gruppo Γ di monodromia, è qui la radice 5.ª $\varepsilon = e^{\frac{2\pi i}{5}}$ dell'unità, che è l'unica irrazionalità nei coefficienti delle sostituzioni del gruppo. È facile quindi vedere quale sarà il gruppo algebrico G, nel campo assoluto di razionalità. Siccome l'equazione irriducibile

$$\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0$$

che definisce ε ha un gruppo d'ordine $= 4$ (§. 94) e G deve contenere Γ come sottogruppo invariante (§. 107), l'ordine m di G sarà dato da

$$m = 4 \times 60 \text{ ovvero } m = 2 \times 60, \; m = 60$$

Ma gli ultimi due casi sono da escludersi perchè, estraendo al massimo una radice quadrata, il quoziente dei due rami x_0, $x_1 = \varepsilon x_0$:

$$\frac{x_1}{x_0} = \varepsilon,$$

rimanendo invariato per tutte le sostituzioni di Γ, sarebbe allora razionalmente noto; basterebbe cioè al massimo l'estrazione di una radice quadrata per conoscere ε, ciò che è assurdo.

§. 118. — L'equazione dell'icosaedro possiede diverse risolventi, della cui formazione vogliamo ora occuparci, premettendo l'osservazione generale che una qualunque di queste risolventi ha un gruppo di monodromia oloedricamente isomorfo col gruppo icosaedrale G_{60}, poichè questo gruppo è semplice.

Le risolventi cercate corrispondono ai diversi sottogruppi di G_{60} ed hanno gradi rispettivamente eguali agli indici dei sottogruppi. Ogni sottogruppo di G_{60}, come gruppo di sostituzioni lineari sopra una variabile, deve rientrare in uno dei cinque tipi del Cap. IV; dopo di ciò è facile l'enumerazione dei diversi tipi possibili di sottogruppi corrispondenti ai divisori di 60, ciò che corrisponde all'enumerazione dei sottogruppi del gruppo alterno su 5 elementi.

Troviamo così come possibili sottogruppi:

1.°	sottogruppi	ciclici	del	2.°	ordine
2.°	„	„	„	3.°	„
3.°	„	„	„	5.°	„
4.°	sottogruppi	diedrali	„	4.°	„
5.°	„	„	„	6.°	„
6.°	„	„	„	10.°	„
7.°	sottogruppi	tetraedrali	„	12.°	„

La loro effettiva esistenza risulta subito dalla ispezione diretta del gruppo dell'icosaedro. Così i sottogruppi diedrali del 10.° ordine sono

quelli che lasciano fisso un diametro dell'icosaedro; essi sono tutti fra loro affini in numero di 6 [1]). I sottogruppi tetraedrali sono quelli che lasciano fisso uno dei cinque ottaedri che hanno per vertici i punti medii delle costole dell'icosaedro; esistono 5 tali sottogruppi fra loro affini [2]).

L'equazione dell'icosaedro possiede quindi risolventi dei rispettivi gradi

$$30\,,\ 20\,,\ 12\,,\ 15\,,\ 10\,,\ 6\,,\ 5\,.$$

Le risolventi dei due ultimi gradi 6, 5 hanno per noi uno speciale interesse e di queste soltanto ci occuperemo. Prescindendo da trasformazioni di Tschirnhaus, esiste manifestamente una sola risolvente di 5.° grado ed una sola di 6.° grado.

Per la formazione effettiva delle risolventi, Klein si serve di un metodo elegante che utilizza le proprietà invariantive e che noi passiamo ora a descrivere, riferendoci, per fissare le idee, alla risolvente di 5.° grado. Scelto uno dei cinque sottogruppi tetraedrali, prendiamo una forma $\varphi_0(z_1, z_2)$ che rimanga invariata per tutte e sole le corrispondenti sostituzioni omogenee tetraedrali. Applicando a questa forma le 120 sostituzioni omogenee icosaedrali, otteniamo $\frac{120}{24} = 5$ forme distinte

$$\varphi_0\,,\ \varphi_1\,,\ \varphi_2\,,\ \varphi_3\,,\ \varphi_4\,,$$

che le sostituzioni icosaedrali permuteranno fra loro secondo le sostituzioni del gruppo alterno. Ora costruiamo il prodotto

$$\prod_{r=0}^{r=4} (\varphi - \varphi_r)\ ,$$

indicando con φ una indeterminata. Nel corrispondente polinomio di 5.° grado

$$\varphi^5 + a\varphi^4 + b\varphi^3 + c\varphi^2 + d\varphi + e = \prod_{r=0}^{r=4} (\varphi - \varphi_r)\ ,$$

---

[1]) Un sottogruppo del 10.° ordine deve contenere una sostituzione ciclica S del 5.° ordine, che è quindi una rotazione attorno ad un diametro dell'icosaedro e le rimanenti debbono trasformare S in una potenza di S e lasciare quindi fisso il medesimo diametro (sottogruppi semimetaciclici).

[2]) Un sottogruppo (tetraedrale) del 12.° ordine contiene un sottogruppo diedrale del 4.° ordine invariante; i tre assi ortogonali delle rotazioni di questo sottogruppo intersecano la sfera in 6 punti che sono i vertici di un ottaedro regolare; le rotazioni del gruppo tetraedrale debbono dunque lasciar fisso questo ottaedro.

i coefficienti a, b, c, d, e, come funzioni simmetriche elementari di φ_0, φ_1, φ_2, φ_3, φ_4, sono forme invarianti icosaedrali e, come tali, funzioni razionali intere di f, H, T, che è facile determinare conoscendo i rispettivi gradi di a, b, c, d, e e i loro coefficienti numerici. Così le 5 forme φ_r sono radici dell'equazione di 5.° grado

$$\varphi^5 + a\varphi^4 + b\varphi^3 + c\varphi^2 + d\varphi + e = 0, \tag{20}$$

i cui coefficienti sono razionali interi in f, H, T.

Per cangiarla ora in una risolvente dell'equazione dell'icosaedro basta moltiplicare o dividere φ per tali potenze di f, H, T da ottenere una funzione omogenea di grado zero in z_1, z_2, cioè una funzione razionale di $z = \frac{z_1}{z_2^4}$.

§. 119. — Cominciamo dall'applicare il metodo invariantivo descritto alla costruzione delle risolventi di 5.° grado. Converrà perciò scegliere una forma $\varphi(z_1, z_2)$ appartenente ad uno dei cinque sottogruppi tetraedrali, p. e. quella di 6.° ordine che ha per radici i vertici di uno dei cinque ottaedri già menzionati. Per costruire una tale forma, che indicheremo con t, e quindi tutte le altre, osserviamo che, per quanto si è visto al §. 49, le tre sostituzioni ivi indicate con

$$\mathrm{T}\ ,\ \mathrm{U}\ ,\ \mathrm{TU}\ ,$$

insieme coll'identità, formano un tale sottogruppo diedrale G_4 e i poli di queste tre sostituzioni sono appunto i 6 vertici di uno degli ottaedri. Ora per queste tre sostituzioni abbiamo la rappresentazione analitica

$$\mathrm{T)} \qquad z' = \frac{(\varepsilon^4 - \varepsilon)z + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3)z - (\varepsilon^4 - \varepsilon)}$$

$$\mathrm{U)} \qquad z' = -\frac{1}{z}$$

$$\mathrm{TU)} \qquad z' = \frac{(\varepsilon^2 - \varepsilon^3)z + (\varepsilon - \varepsilon^4)}{(\varepsilon - \varepsilon^4)z - (\varepsilon^2 - \varepsilon^3)}$$

e quindi le forme di 2.° grado che hanno le radici nei loro poli sono

le seguenti [1]:

$$\begin{cases} z_1^2 - 2(\varepsilon^2 + \varepsilon^3) z_1 z_2 - z_2^2 \\ z_1^2 + z_2^2 \\ z_1^2 - 2(\varepsilon + \varepsilon^4) z_1 z_2 - z_2^2 . \end{cases}$$

Possiamo prendere t semplicemente eguale al prodotto di queste tre forme, onde risulta:

$$t = (z_1^2 + z_2^2)(z_1^4 + 2 z_1^3 z_2 - 6 z_1^2 z_2^2 - 2 z_1 z_2^3 + z_2^4) ,$$

ovvero

$$t = z_1^6 + 2 z_1^5 z_2 - 5 z_1^4 z_2^2 - 5 z_1^2 z_2^4 - 2 z_1 z_2^5 + z_2^6 . \tag{21}$$

Una seconda forma che rimane ancora invariata per le sostituzioni del detto sottogruppo tetraedrale è quella che ha per indici delle radici gli 8 punti medii delle facce dell'ottaedro considerato (proiettati dal centro sulla sfera). Mediante considerazioni perfettamente simili a quelle del §. 116, vediamo che la detta forma dell'8.° grado W sarà, a meno di un fattore, la forma Hessiana della t. Poniamo

$$W = \frac{1}{4^2 . 5^2} \begin{vmatrix} \dfrac{\partial^2 t}{\partial z_1^2} & \dfrac{\partial^2 t}{\partial z_1 \partial z_2} \\ \dfrac{\partial^2 t}{\partial z_2 \partial z_1} & \dfrac{\partial^2 t}{\partial z_2^2} \end{vmatrix}$$

e troveremo:

$$W = -(z_1^8 + z_2^8) + (z_1^7 z_2 - z_1 z_2^7) - 7(z_1^6 z_2^2 - z_1^2 z_2^6) - 7(z_1^5 z_2^3 - z_1^3 z_2^5) . \tag{22}$$

Qualunque altra forma invariabile per le sostituzioni del sottogruppo tetraedrale in considerazione si esprimerà per le due fondamentali t e W (Cf. §. 115). Per le 60 rotazioni dell'icosaedro, ovvero per le 120 sostituzioni del gruppo omogeneo icosaedrale [2]), le nostre forme t, e W

---

[1]) Si abbia riguardo alle formule:

$$\varepsilon^4 - \varepsilon = (\varepsilon^2 - \varepsilon^3)(\varepsilon^2 + \varepsilon^3)$$
$$\varepsilon^2 - \varepsilon^3 = (\varepsilon - \varepsilon^4)(\varepsilon + \varepsilon^4).$$

[2]) Si noti che t, W, come forme di grado pari, restano invariate cangiando i segni di z_1, z_2.

si mutano rispettivamente in 5 forme distinte che otteniamo applicando le potenze S^r della sostituzione fondamentale S, cioè, sotto forma omogenea, le sostituzioni

$$S^r) \quad z'_1 = \pm \varepsilon^{3r} z_1 , \; z'_2 = \pm \varepsilon^{2r} z_2$$
$$(r = 0, 1, 2, 3, 4).$$

Indicando i rispettivi valori di t, W con t_r, W_r, avremo

$$(21^*) \qquad t_r = \varepsilon^{3r} z_1^6 + 2\,\varepsilon^{2r} z_1^5 z_2 - 5\,\varepsilon^r z_1^4 z_2^2 - 5\,\varepsilon^{4r} z_1^2 z_2^4 - 2\,\varepsilon^{3r} z_1 z_2^5 + \varepsilon^{2r} z_2^6$$

$$(22^*) \qquad W_r = -\varepsilon^{4r} z_1^8 + \varepsilon^{3r} z_1^7 z_2 - 7\,\varepsilon^{2r} z_1^6 z_2^2 - 7\,\varepsilon^r z_1^5 z_2^2 + 7\,\varepsilon^{4r} z_1^3 z_2^5 -$$
$$- 7\,\varepsilon^{3r} z_1 z_2^7 - \varepsilon^r z_2^8 .$$

Le 60 rotazioni dell'icosaedro permuteranno fra loro le cinque forme t_r e le W_r precisamente come i cinque ottaedri corrispondenti e se ci riportiamo alla rappresentazione geometrica del §. 55, osservando che le denominazioni ivi date A, B, C, D, E pei cinque ottaedri corrispondono agli attuali indici 0, 1, 2, 3, 4, ne deduciamo che la rotazione elementare S produce sulle forme t o W la sostituzione ciclica del 5.° ordine

$$(t_0\, t_1\, t_2\, t_3\, t_4) \text{ o } (W_0\, W_1\, W_2\, W_3\, W_4)$$

e la rotazione elementare T i prodotti di due trasposizioni

$$(t_1\, t_2)\,(t_3\, t_4) \text{ o } (W_1\, W_2)\,(W_3\, W_4) ,$$

restando fissa t_0 o W_0.

§. 120. — Calcoliamo ora in primo luogo, secondo il §. 118 formola (20), i coefficienti della equazione di 5.° grado

$$t^5 + a\,t^4 + b\,t^3 + c\,t^2 + d\,t + e = 0 ,$$

le cui radici sono le forme t_0, t_1, t_2, t_3, t_4.

Osservando che a, b, c, d, e sono forme icosaedrali dei rispettivi gradi

$$6,\ 12,\ 18,\ 24,\ 30,$$

se ne dedurrà subito

$$a = 0,\ b = k\,f,\ c = 0,\ d = l\,f^2,\ e = m\,T ,$$

essendo k, l, m coefficienti numerici, sicchè l'equazione sarà

$$t^5 + k f t^3 + l f^2 t + m \mathrm{T} = 0 .$$

Per determinare k, l, m facciamo $z_2 = 1$, $z_1 = z$ e questa dovrà cangiarsi nell'identità:

$$(z^6+2z^5-5z^4-5z^2-2z+1)^5 + k z (z^{10}+11z^5-1)(z^6+2z^5-5z^4-5z^2-2z+1)^3 +$$
$$+ l z^2 (z^{10}+11z^5-1)^2 (z^6+2z^5-5z^4-5z^2-2z+1) +$$
$$+ m (z^{30}+522z^{25}-10005z^{20}-10005z^{10}-522z^5+1) = 0 .$$

Basta osservare il termine costante per dedurne $m = -1$ e i coefficienti dei termini in $z_1 z_2$ danno i valori di k, l

$$k = -10 , \quad l = 45 ,$$

sicchè l'equazione richiesta si scrive:

$$t^5 - 10 f t^3 + 45 f^2 t - \mathrm{T} = 0 . \tag{23}$$

Per cangiare questa in una risolvente icosaedrale basterà (§. 118) moltiplicare e dividere t per tali potenze di f, H, T da cangiarla in una forma di grado zero in z_1, z_2. Poniamo per ciò

$$u = \frac{12 f^2 t}{\mathrm{T}} ,$$

con che appunto risulterà u funzione di $z = \frac{z_1}{z_2}$ e la (23), avendo riguardo all'equazione (I*) §. 117 dell'icosaedro, diventa:

$$48 u^5 (1 - \mathrm{Z})^2 - 40 u^3 (1 - \mathrm{Z}) + 15 u - 12 = 0 . \tag{III}$$

Questa è la risolvente di 5.° grado dell'equazione dell'icosaedro che Klein chiama la *risolvente delle u* [1]).

Una seconda risolvente, *la risolvente delle r*, si ottiene ponendo

$$r = \frac{t^2}{f} .$$

---

[1]) Klein *l. c.*, pag. 104.

Per calcolarla scriviamola (23) così:

$$T = t\,(t^4 - 10\,f\,t^2 + 45\,f^2)\,,$$

e quadrando, poi dividendo per f^5 col sostituire a $\frac{t^2}{f}$ la r, abbiamo

$$\text{(III*)} \qquad r\,(r^2 - 10\,r + 45)^2 + 12^3\,(Z - 1) = 0,$$

che è la risolvente delle r.

Quale è il gruppo di queste risolventi?

Quanto al gruppo di monodromia esso è il gruppo alterno G_{60} sulle cinque radici, come risulta dai teoremi generali §. 118. Il gruppo algebrico nel campo assoluto di razionalità sarà G_{60} stesso ovvero il gruppo totale G_{120} sulle 5 radici. Per decidere la questione basta considerare la radice quadrata del discriminante della (III) o (III*), che, essendo invariabile per il gruppo G_{60} di monodromia, sarà certo razionale nel parametro Z e i coefficienti saranno numeri razionali se G_{60} è anche il gruppo algebrico e dovranno invece contenere, come irrazionalità numerica, la radice quadrata di un numero razionale nel caso opposto. Ora se costruiamo la radice quadrata del discriminante della (23), cioè

$$\prod_{r<s} (t_r - t_s),$$

basterà osservarne un valore numerico speciale, p. e. quello per $z_2 = 1$, $z_1 = 0$. Siccome t_r diventa allora ε^{2r}, questo valore numerico non differisce dalla radice quadrata del discriminante dell'equazione

$$x^4 + x^3 + x^2 + x + 1 = 0$$

che contiene l'irrazionalità $\sqrt{5}$ (§. 99).

Dunque: *Le risolventi di 5.° grado* (III), (III*) *dell'equazione dell'icosaedro hanno, nel campo assoluto di razionalità, per gruppo algebrico il gruppo totale; questo si abbassa al gruppo alterno, che è il gruppo di monodromia, per l'aggiunta di* $\sqrt{5}$.

§. 121. — Per la risoluzione della equazione generale di 5.° grado mediante la irrazionalità icosaedrica hanno grande importanza quelle speciali risolventi di 5.° grado dell'icosaedro in cui mancano la quarta

e la terza potenza dell'incognita e di queste appunto vogliamo ora occuparci.

Appartiene a questa specie l'equazione che ha per radici

$$W_0, W_1, W_2, W_3, W_4,$$

giacchè ΣW_r e ΣW_r^2, non esistendo forme icosaedrali di 8.° e di 16.° grado, sono identicamente nulle. Lo stesso dicasi della risolvente che ha per radici i prodotti

$$t_0 W_0, t_1 W_1, t_2 W_2, t_3 W_3, t_4 W_4,$$

giacchè non esistono forme icosaedrali dei gradi 14 e 28. Ma si ha anche

$$\sum W_r \,.\, \sum t_r W_r = 0$$

perchè il primo membro è una forma icosaedrale di grado = 22, quindi identicamente nulla. Ne deduciamo che ponendo

$$Y_r = \sigma W_r + \tau t_r W_r, \tag{24}$$

con σ, τ costanti arbitrarie, anche l'equazione di 5.° grado che ha per radici

$$Y_0, Y_1, Y_2, Y_3, Y_4$$

mancherà della 4.ª e 3.ª potenza. Volendo calcolare effettivamente la corrispondente equazione, che scriveremo

$$Y^5 + 5\alpha Y^2 + 5\beta Y + \gamma = 0,$$

cominciamo dall'osservare che si ha

$$\gamma = -\prod_{r=0}^{r=4} (\sigma W_r + \tau t_r W_r) = -\prod_{r=0}^{r=4} (W_r) \,.\, \prod_{r=0}^{r=4} (\sigma + \tau t_r).$$

Ora $\Pi\,(W_r)$ è una forma icosaedrale di grado 40 e, per la formola (a) §. 115, non potrà differire da H^2 che per un coefficiente numerico; troviamo quindi subito

$$\Pi\,(W_r) = -H^2.$$

D'altronde dalla (23) §. 120, indicando con λ un'arbitraria, ricaviamo l'identità

$$\lambda^5 - 10 f \lambda^3 + 45 f^2 \lambda - T = \prod_r (\lambda - t_r),$$

onde, facendo $\lambda = -\frac{\sigma}{\tau}$, risulta

$$\prod_r (\sigma + \tau t_r) = \sigma^5 - 10 f \sigma^3 \tau^2 + 45 f^2 \sigma \tau^4 + T \tau^5$$

e però

$$\gamma = H^2 [\sigma^5 - 10 f \sigma^3 \tau^2 + 45 f^2 \sigma \tau^4 + T \tau^5].$$

Per calcolare poi α, β ricorriamo p. e. alle formole di Newton che danno

$$-15 \alpha = \sum (\sigma W_r + \tau t_r W_r)^3$$

$$-20 \beta = \sum (\sigma W_r + \tau t_r W_r)^4 .$$

Sviluppando le espressioni dei secondi membri per potenze di σ, τ, osservando i gradi delle corrispondenti forme icosaedrali che ne sono i coefficienti, si trova

$$\alpha = 8 f^2 \sigma^3 + T \sigma^2 \tau + 72 f^3 \sigma \tau^2 + f T . \tau^3$$

$$\beta = -f H \sigma^4 + 18 f^2 H \sigma^2 \tau^2 + H T \sigma \tau^3 + 27 f^3 H \tau^4.$$

Per cangiare nuovamente l'equazione di 5.° grado nelle Y in una risolvente icosaedrale, poniamo come sopra

(25) $$u = \frac{12 f^2 t}{T}$$

e inoltre

(25*) $$v = \frac{12 f W}{H} ;$$

allora la (24) si scrive

(26) $$Y_r = m v_r + n u_r v_r ,$$

ove si ponga

(27) $$m = \frac{\sigma H}{12 f}, \; n = \frac{\tau H T}{12^2 . f^2} .$$

Sostituendo i valori che ne risultano per σ, τ nella equazione in Y, questa diventa:

$$\text{(IV)} \qquad Z\,Y^5 + 5\,Y^2\left(8\,m^3 + 12\,m^2\,n + \frac{6\,m\,n^2 + n^3}{1 - Z}\right) +$$

$$+ 15\,Y\left(-4\,m^4 + \frac{6\,m^2 n^2 + 4\,m\,n^3}{1 - Z} + \frac{3\,n^4}{(1-Z)^2}\right) +$$

$$+ 3\left(48\,m^5 - \frac{40\,m^3\,n^2}{1 - Z} + \frac{15\,m\,n^4 + 4\,n^5}{(1 - Z)^2}\right) = 0\,.$$

Questa dicesi, secondo KLEIN, la *risolvente principale* di 5.° grado della equazione dell'icosaedro [1]).

Per la determinazione del suo gruppo valgono le considerazioni stesse del §. precedente. Il suo gruppo algebrico nel campo assoluto di razionalità, cui siano aggiunte m, n, è il gruppo totale sulle 5 radici. Per l'aggiunta di $\sqrt{5}$ questo si abbassa al gruppo alterno, che è il gruppo di monodromia.

Le risolventi di 5.° grado (III), (III*), (IV) sopra determinate sono naturalmente tutte trasformate di TSCHIRNHAUS l'una dell'altra e si potrebbero facilmente trovare le formole che esprimono razionalmente u e Y per r [2]).

§. 122. — Occupiamoci ora di costruire una risolvente di 6.° grado. Prendiamo perciò come forma di 4.° grado invariabile per un sottogruppo diedrale G_{10} semplicemente la seguente

$$\varphi = 5\,z_1^2\,z_2^2,$$

che ha i punti radici nelle estremità del diametro congiungente i poli $z = 0$, $z = \infty$ e rimane quindi invariata per il sottogruppo diedrale [3])

$$G_{10} = \begin{cases} 1,\ S,\ S^2,\ S^3,\ S^4 \\ U,\ US,\ US^2,\ US^3,\ US^4\,. \end{cases}$$

---

[1]) KLEIN, *l. c.* pag. 106.

[2]) KLEIN, *l. c.* pag. 106.

[3]) Si osservi che il prodotto semplice $z_1\,z_2$, che sembrerebbe più naturale di considerare, per la sostituzione U che, scritta sotto forma omogenea è $z'_1 = \pm\,z_2$, $z'_2 = \mp\,z_1$ cangerebbe di segno.

Applicando alla φ la sostituzione omogenea sotto la forma (13*) §. 114), ne otterremo la nuova forma

$$\varphi_0 = (z_1^2 + z_1 z_2 - z_2^2)^2,$$

che per la S^r si cangia in generale in

$$\varphi_r = (\varepsilon^r z_1^2 + z_1 z_2 - \varepsilon^{4r} z_2^2)^2.$$

Contraddistinguendo il valore iniziale di φ con

$$\varphi_\infty = 5\, z_1^2 z_2^2,$$

costruiamo l'equazione di 6.° grado

$$\varphi^6 + a'\varphi^5 + b'\varphi^4 + c'\varphi^3 + d'\varphi^2 + e'\varphi + f' = 0,$$

che ha per radici

$$\varphi_\infty, \varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4.$$

I suoi coefficienti $a'\, b' \ldots$ nell'ordine scritto saranno forme icosaedrali dei gradi rispettivi

$$4,\ 8,\ 12,\ 16,\ 20,\ 24$$

e però si avrà

$$a' = b' = d' = 0,\ c' = hf,\ e' = k\mathrm{H},\ f' = l f^2,$$

con h, k, l coefficienti numeri che determiniamo subito osservando l'identità che ne risulta:

$$5^6 z^{12} + 5^3 z^6 . h z (z^{10} + 11 z^5 - 1) + 5 k z^2 (-z^{20} + 228 z^{15} - 494 z^{10} - 228 z^5 - 1) + \\ + l z^2 (z^{10} + 11 z^5 - 1)^2 = 0$$

ovvero, posto $z^5 = \xi$:

$$5^6 \xi^2 + 5^3 h \xi (\xi^2 + 11 \xi - 1) + 5 k (-\xi^4 + 228 \xi^3 - 494 \xi^2 - 228 \xi - 1) + \\ + l (\xi^2 + 11 \xi - 1)^2 = 0,$$

onde segue

$$h = -10,\ k = 1,\ l = 5.$$

Troviamo così per φ l'equazione:

$$\varphi^6 - 10 f \varphi^3 + H \varphi + 5 f^2 = 0 ,$$

che cangiamo in una risolvente icosaedrale ponendo

$$\zeta = \frac{H \varphi}{12 f^2} ;$$

sostituendo otteniamo per la risolvente domandata

$$\text{(V)} \qquad \zeta^6 - 10 Z \zeta^3 + 12 Z^2 \zeta + 5 Z^2 = 0 .$$

Quale sarà il gruppo di questa risolvente?

Quanto al gruppo di monodromia esso è il gruppo indotto sulle radici

$$\varphi_\infty , \ \varphi_0 , \ \varphi_1 , \ \varphi_2 , \ \varphi_3 , \ \varphi_4$$

dalle 60 rotazioni dell'icosaedro, cioè il *gruppo modulare* sulle 6 radici (Cf. §. 55). Del resto, calcolando direttamente l'effetto prodotto dalle rotazioni elementari S, T, troviamo che la S produce la sostituzione ciclica

$$(\varphi_0 \ \varphi_1 \ \varphi_2 \ \varphi_3 \ \varphi_4)$$

lasciando ferma φ_∞, mentre la T produce il prodotto di due trasposizioni

$$(\varphi_0 \ \varphi_\alpha) \ (\varphi_1 \ \varphi_4)$$

lasciando fisse φ_2, φ_3. Queste sono le due sostituzioni elementari

$$\nu' \equiv \nu + 1 , \ \nu' \equiv -\frac{1}{\nu} \pmod 5$$

del gruppo modulare. Quanto al gruppo algebrico della (V) nel campo assoluto di razionalità, dovendo esso contenere il gruppo modulare come sottogruppo invariante, pel teorema alla fine del §. 42, non potrà essere che il gruppo modulare stesso, ovvero il gruppo lineare totale di 120 sostituzioni

$$\nu' \equiv \frac{\alpha \nu + \beta}{\gamma \nu + \delta} , \ \alpha\delta - \beta\gamma \not\equiv 0 \pmod 5 .$$

Per decidere l'alternativa si consideri la radice quadrata del discriminante della equazione (V) e se ne calcoli il valore numerico p. e. per $z = 1$, il che dà

$$\varphi_\infty = 0, \quad \varphi_r = \varepsilon^{2r}$$

e si vedrà subito che esso contiene l'irrazionalità quadratica $\sqrt{5}$. Concludiamo adunque:

Il gruppo algebrico della risolvente (V) *di 6.° grado, nel campo assoluto di razionalità, è il gruppo lineare totale sui 6 indici* ∞, 0, 1, 2, 3, 4; *questo si abbassa al gruppo modulare, che è il gruppo di monodromia, per l'aggiunta di* $\sqrt{5}$.

§. 123. — L'equazione di 5.° grado (IV) §. 121 è un'equazione *principale*, indicando con questa denominazione le equazioni di 5.° grado mancanti dei termini colla 4.ª e 3.ª potenza della incognita. Se al campo di razionalità dei coefficienti della (IV) si aggiunge $\sqrt{5}$ la radice quadrata del discriminante risulta razionalmente nota e l'equazione dell'icosaedro viene ad essere precisamente la risolvente di Galois della (V). Ora vogliamo inversamente ricercare se prendendo un'equazione principale qualunque di 5.° grado:

$$y^5 + 5\,\alpha\, y^2 + 5\,\beta\, y + \gamma = 0 \tag{28}$$

ed aggiungendo al campo di razionalità la radice quadrata del suo discriminante ∇, sarà possibile costruire una risolvente di Galois che sia precisamente un'equazione icosaedrale.

Ma dimostriamo in primo luogo che l'equazione *generale* di 5.° grado si può sempre ridurre alla forma principale (28), estraendo soltanto una radice quadrata. Della equazione data di 5.° grado.

$$x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5 = 0$$

costruiamo una trasformata di Tschirnhaus ponendo

$$y = \alpha_1 + \alpha_2 x + \alpha_3 x^2$$

e sia

$$y^5 + A_1 y^4 + A_2 y_3 + A_3 y^2 + A_4 y + A_5 = 0.$$

Si tratta di fare in modo che risulti

$$A_1 = 0\,,\ A_2 = 0\,;$$

e siccome A_1, A_2 sono funzioni intere omogenee nelle α di 1.° e 2.° grado rispettivamente, è chiaro che potremo prendere le α nel modo richiesto, risolvendo soltanto un'equazione di 2.° grado.

Ed ora all'oggetto di costruire una risolvente icosaedrale della equazione principale data (28), converrà esaminare come per la equazione principale (IV) questa risolvente icosaedrale è effettivamente costruita, in qual modo cioè la radice $z = \frac{z_1}{z_2}$ dell'equazione dell'icosaedro è espressa razionalmente per le radici

$$Y_0,\ Y_1,\ Y_2,\ Y_3,\ Y_4$$

della (IV). Per ciò dalle formole (21*) (22*) per W_r, t_r (§. 119) deduciamo

$$W_r = (\varepsilon^{4r} z_1 - \varepsilon^{3r} z_2)\,(7\, z_1^2 z_2^5 - z_1^7) - (\varepsilon^{2r} z_1 + \varepsilon^r z_2)\ (z_2^7 + 7\, z_1^5 z_2^2)$$

$$t_r\, W_r = (\varepsilon^{4r} z_1 - \varepsilon^{3r} z_2)\ (-26\, z_1^{10} z_2^3 + 39\, z_1^5 z_2^8 + z_2^{13} -$$

$$-(\varepsilon^{2r} z_1 + \varepsilon^r z_2)\ (z_1^{13} - 39\, z_1^8 z_2^5 - 26\, z_1^3 z_2^{10})\,,$$

onde segue che la Y_r, data dalla (24) §. 121, assume la forma

$$Y_r = (\varepsilon^{4r} z_1 - \varepsilon^{3r} z_2)\ R + (\varepsilon^{2r} z_1 + \varepsilon^r z_2)\, S\,,$$

essendo R, S espressioni lineari in σ, τ.

Ora costruiamo le due espressioni seguenti

$$(\varepsilon,\ Y_0) = Y_0 + \varepsilon\ Y_1 + \varepsilon^2 Y_2 + \varepsilon^3 Y_3 + \varepsilon^4 Y_4$$
$$(\varepsilon^2,\ Y_0) = Y_0 + \varepsilon^2 Y_1 + \varepsilon^4 Y_2 + \varepsilon\ Y_3 + \varepsilon^3 Y_4$$

e ne dedurremo

$$\begin{cases} Y_0 + \varepsilon\ Y_1 + \varepsilon^2 Y_2 + \varepsilon^3 Y_3 + \varepsilon^4 Y_4 = 5\, z_1 R \\ Y_0 + \varepsilon^2 Y_1 + \varepsilon^4 Y_2 + \varepsilon\ Y_3 + \varepsilon^3 Y_4 = -5\, z_2 R, \end{cases}$$

da cui la formula cercata

$$(29) \qquad z = \frac{z_1}{z_2} = -\frac{Y_0 + \varepsilon\ Y_1 + \varepsilon^2 Y_2 + \varepsilon^3 Y_3 + \varepsilon^4 Y_4}{Y_0 + \varepsilon^2 Y_1 + \varepsilon^4 Y_2 + \varepsilon\ Y_3 + \varepsilon^3 Y_4}\,,$$

che esprime la radice x della risolvente icosaedrale per le radici della equazione principale di 5.° grado (IV).

Poichè, come si è visto al §. 119, alle rotazioni elementari S, T dell'icosaedro corrispondono rispettivamente le sostituzioni

$$(Y_0\, Y_1\, Y_2\, Y_3\, Y_4),\quad (Y_1\, Y_2)\,(Y_3\, Y_4)$$

sulle radici Y_r, inversamente ne segue che se nella espressione (29) della z si eseguiscono queste permutazioni elementari del gruppo alterno sulle Y, la z subirà le due sostituzioni elementari del gruppo icosaedrale.

$$z' = \varepsilon z\ ,\quad z' = \frac{(\varepsilon^4 - \varepsilon)\, z + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3)\, z - (\varepsilon^4 - \varepsilon)}\ ,$$

Notiamo subito che mentre la prima formola, e cioè:

$$\frac{Y_1+\varepsilon\ Y_2+\varepsilon^2\, Y_3+\varepsilon^3\, Y_4+\varepsilon^4\ Y_0}{Y_1+\varepsilon^2\, Y_2+\varepsilon^4\, Y_3+\varepsilon\ Y_4+\varepsilon^3\, Y_0} = \varepsilon\, \frac{Y_0+\varepsilon\ Y_1+\varepsilon^2\, Y_2+\varepsilon^3\, Y_3+\varepsilon^4\, Y_4}{Y_0+\varepsilon^2\, Y_1+\varepsilon^4\, Y_2+\varepsilon\ Y_3+\varepsilon^3\, Y_4}$$

sussisterebbe anche se le Y fossero fra loro indipendenti, la seconda invece non è un'identità nelle Y e sussiste soltanto in forza delle relazioni

$$\sum Y_r = 0\ ,\quad \sum Y_r^2 = 0.$$

§. 124. — I risultati precedenti conducono naturalmente a ricercare se per un'equazione principale di 5.° grado qualsiasi

$$y^5 + 5\,\alpha\, y^2 + 5\,\beta\, y + \gamma = 0 \tag{28}$$

accade quello che abbiamo visto verificarsi per la (IV), se cioè la funzione razionale delle radici data dalla formola

$$\lambda = -\frac{y_0+\varepsilon\, y_1+\varepsilon^2\, y_2+\varepsilon^3 y_3+\varepsilon^4\, y_4}{y_0+\varepsilon^2 y_1+\varepsilon^4\, y_2+\varepsilon\ y_3+\varepsilon^3\, y_4}\ , \tag{30}$$

per le 60 sostituzioni del gruppo alterno sulle y, subisce le 60 sostituzioni del gruppo icosaedrale e in particolare per le due sostituzioni elementari:

$$(y_0\, y_1\, y_2\, y_3\, y_4)\quad ,\quad (y_1\, y_2)\,(y_3\, y_4)$$

del gruppo alterno subisce le sostituzioni generatrici S, T del gruppo dell'icosaedro:

$$\text{S)}\ \lambda' = \varepsilon\lambda \quad , \quad \text{T)}\ \lambda' = \frac{(\varepsilon^4 - \varepsilon)\lambda + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3)\lambda - (\varepsilon^4 - \varepsilon)} .$$

Quanto alla prima sostituzione si è già osservato sopra che ciò ha luogo infatti, anzi indipendentemente dalle relazioni

$$(b) \qquad \sum y_r = 0 \quad , \quad \sum y_r^2 = 0 ,$$

cui soddisfano le y. Per la seconda la verifica riesce alquanto più complicata, dovendosi tener conto delle due relazioni (b). Introduciamo perciò le 5 espressioni

$$(\varepsilon^r , y_0) = \sum_{s=0}^{s=4} \varepsilon^{rs} y_s \quad (r = 0, 1, 2, 3, 4) ,$$

che figurano come funzioni trasformatrici per la risolvente di Lagrange e delle quali la prima $(1, y_0)$ è nulla a causa della prima delle (b). Poniamo

$$(\varepsilon^r , y_0) = 5\,\xi_r \quad (r = 0, 1, 2, 3, 4) ,$$

ove la ξ_0 sarà $= 0$ e risolvendo questo sistema lineare rispetto alle y, avremo

$$(31) \qquad y_r = \varepsilon^{4r}\xi_1 + \varepsilon^{3r}\xi_2 + \varepsilon^{2r}\xi_3 + \varepsilon^r \xi_4$$
$$(r = 0, 1, 2, 3, 4)$$

e la 2.ª relazione (b) $\sum y_r^2 = 0$ diventerà nelle ξ:

$$(32) \qquad \xi_1 \xi_4 + \xi_2 \xi_3 = 0 .$$

Ora indichiamo con $\bar{\xi}_1, \bar{\xi}_2$ i valori che assumono ξ_1, ξ_2 dopo eseguita la permutazione

$$(y_1\, y_2)\ \ (y_3\, y_4)$$

ed avremo

$$\begin{cases} 5\,\bar{\xi}_1 = y_0 + \varepsilon^2 y_1 + \varepsilon\, y_2 + \varepsilon^4 y_3 + \varepsilon^3 y_4 \\ 5\,\bar{\xi}_2 = y_0 + \varepsilon^4 y_1 + \varepsilon^2 y_2 + \varepsilon^3 y_3 + \varepsilon\, y_4 , \end{cases}$$

ossia per le (31):

$$(33)\quad \begin{cases} 5\,\bar{\xi}_1 = [2\,(\varepsilon+\varepsilon^4)+1]\,\xi_1 + [(\varepsilon^2+\varepsilon^3)+3]\,\xi_2 + [(\varepsilon+\varepsilon^4)+3]\,\xi_3 + \\ \qquad\qquad + [2\,(\varepsilon^2+\varepsilon^3)+1]\,\xi_4 \\ 5\,\bar{\xi}_2 = [(\varepsilon^2+\varepsilon^3)+3]\,\xi_1 + [2\,(\varepsilon^2+\varepsilon^3)+1]\,\xi_2 + [2\,(\varepsilon+\varepsilon^4)+1]\,\xi_3 + \\ \qquad\qquad + [(\varepsilon+\varepsilon^4)+3]\,\xi_4\,. \end{cases}$$

D'altronde il valore trasformato di λ essendo

$$\lambda' = -\frac{\bar{\xi}_1}{\bar{\xi}_2}\,,$$

la formola da verificarsi

$$\lambda' = \frac{(\varepsilon^4-\varepsilon)\,\lambda + \varepsilon^2-\varepsilon^3}{(\varepsilon^2-\varepsilon^3)\,\lambda - (\varepsilon^4-\varepsilon)}$$

diventa:

$$(\varepsilon-\varepsilon^4)\,\xi_1\,\bar{\xi}_2 + (\varepsilon^2-\varepsilon^3)\,\xi_2\,\bar{\xi}_2 - (\varepsilon^2-\varepsilon^3)\,\xi_1\,\bar{\xi}_1 + (\varepsilon-\varepsilon^4)\,\xi_2\,\bar{\xi}_1 = 0\,,$$

la quale, pei valori (33) di $\bar{\xi}_1$, $\bar{\xi}_2$, si riduce alla seguente

$$5\,(\varepsilon-\varepsilon^4)\,(\xi_1\,\xi_4+\xi_2\,\xi_3) = 0\,,$$

che è verificata per la (32).

Così dunque la funzione razionale λ, data dalla (30), delle radici della proposta (28) subisce per le sostituzioni del gruppo alterno sulle y le 60 sostituzioni lineari del gruppo icosaedrale e per conseguenza se costruiamo l'equazione icosaedrale

$$(34)\qquad \frac{(\lambda^{20}-228\,\lambda^{15}+494\,\lambda^{10}+228\,\lambda^5+1)^3}{12^3\,\lambda^5\,(\lambda^{10}+11\,\lambda^5-1)^5} = Z,$$

o, più brevemente:

$$(34^*)\qquad \frac{H^3(\lambda)}{12^3\,f^5(\lambda)} = Z\,,$$

le cui radici sono i 60 valori di λ

$$\lambda_1\,,\ \lambda_2 \ldots \lambda_{60}\,,$$

il secondo membro Z, come funzione simmetrica di questi 60 valori, sarà una funzione semisimmetrica di y_0, y_1, y_2, y_3, y_4 e però razionalmente

esprimibile per α, β, γ e $\sqrt{\Delta}$ [1]). La (34) o (34*) è quindi, come si voleva, una risolvente di GALOIS icosaedrale della equazione principale proposta (28).

§. 125. — Le considerazioni del §. precedente ci hanno dimostrato la possibilità di costruire una risolvente di GALOIS icosaedrale per la equazione principale di 5.° grado e quindi in sostanza la possibilità di risolvere l'equazione generale di 5.° grado coll'aggiunta di radicali quadrati e di un'irrazionalità icosaedrica.

Ma per dare le effettive formole di risoluzione possiamo seguire in certo modo un cammino inverso e cioè identificare, come deve pure essere possibile, la risolvente principale delle Y (IV), §. 121 dell'equazione dell'icosaedro con un'equazione principale (28) di 5.° grado data ad arbitrio, disponendo convenientemente di m, n, Z che debbono potersi esprimere razionalmente per

$$\alpha\,,\ \beta\,,\ \gamma\,,\ \sqrt{\nabla}\,.$$

Il calcolo che resta da farsi si eseguirà nel modo seguente [2]). Il paragone della (IV) colla (28) fornisce le tre equazioni

$$(35)\qquad \left\{\begin{aligned} Z\alpha &= 8m^3 + 12\,m^2 n + \frac{6\,m\,n^2 + n^3}{1-Z} \\ \frac{Z\beta}{3} &= -\,4m^4 + \frac{6\,m^2 n^2 + 4\,m\,n^3}{1-Z} + \frac{3\,n^4}{4\,(1-Z)^2} \\ \frac{Z\gamma}{3} &= 48\,m^5 - \frac{40\,m^3 n^2}{1-Z} + \frac{15\,m\,n^4 + 4\,n^5}{(1-Z)^2} \end{aligned}\right.$$

dalle quali deduciamo, con semplice calcolo, le tre seguenti

$$(36)\qquad \frac{12\,\beta\,m + \gamma}{12\,\alpha} = \frac{n^2}{1-Z}$$

$$(37)\qquad m\,\gamma - \frac{n^2\beta}{1-Z} = \frac{9}{4Z}\left(4\,m^2 - \frac{n^2}{1-Z}\right)^3$$

$$(38)\qquad \alpha^2 - \frac{4}{81}\,\frac{1-Z}{n^2}\,(3\,m\,\alpha + 2\,\beta)^2 = \frac{1}{Z}\left(4\,m^2 - \frac{n^2}{1-Z}\right)^3.$$

---

[1]) Per il calcolo effettivo di Z in funzione razionale di α, β, γ, $\sqrt{\nabla}$ veggasi: KLEIN *l. c.*, pag. 194 e ss.

[2]) KLEIN *l. c.*, pag. 192 e ss.

Dal confronto delle due ultime deduciamo

$$\alpha^2 - \frac{4}{81}\,\frac{1-Z}{n^2}\,(3\,m\,\alpha + 2\,\beta)^2 = \frac{4}{9}\left(m\gamma - \frac{n^2\beta}{1-Z}\right)$$

e, sostituendo in questa per $\frac{n^2}{1-Z}$ il valore dato dalla (36), otteniamo la seguente equazione di 2.° grado per determinare m:

$$16\,(\alpha^4 - \beta^3 + \alpha\,\beta\,\gamma)\,m^2 - \frac{4}{3}(11\,\alpha^3\,\beta + 2\,\beta^2\,\gamma - \alpha\,\gamma^2)\,m + \frac{1}{9}(64\,\alpha^2\,\beta^2 - 27\,\alpha^3\gamma - \beta\gamma^2) = 0.$$

La risoluzione di questa equazione di 2.° grado ci dà per m il valore

$$m = \frac{11\,\alpha^3\,\beta + 2\,\beta^2\,\gamma - \alpha\,\gamma^2 \pm \alpha\sqrt{\nabla}}{24\,(\alpha^4 - \beta^3 + \alpha\,\beta\,\gamma)}\,, \tag{39}$$

avendo posto

$$\nabla = 108\,\alpha^5\,\gamma - 135\,\alpha^4\,\beta^2 + 90\,\alpha^2\,\beta\,\gamma^2 - 320\,\alpha\,\beta^3\,\gamma + 256\,\beta^5 + \gamma^4, \tag{40}$$

valore che differisce dal discriminante della proposta (28) solo per un coefficiente numerico [1]).

Calcolato il valore di m dalla (39) collo scegliere l'una o l'altra delle due determinazioni di segno per $\sqrt{\nabla}$, ne dedurremo poi razionalmente Z, n colle osservazioni seguenti.

Sostituendo nella (37) per $\frac{n^2}{1-Z}$ il valore dato dalla (36) abbiamo:

$$Z = \frac{(48\,\alpha\,m^2 - 12\,\beta\,m - \gamma)^3}{64\,\alpha^2[12\,(\alpha\,\gamma - \beta^2)\,m - \beta\,\gamma]}\,, \tag{41}$$

formola che ci determina Z. In fine per determinare n scriviamo la prima delle (35) così:

$$\left(12\,m^2 + \frac{n^2}{1-Z}\right)n = \alpha\,Z - 8\,m^3 - 6\,m\,\frac{n^2}{1-Z}$$

e ponendovi per $\frac{n^2}{1-Z}$ il valore (36), avremo la formola finale:

$$n = \frac{12\,\alpha^2\,Z - 96\,\alpha\,m^3 - 72\,\beta\,m^2 - 6\,\gamma\,m}{144\,\alpha\,m^2 + 12\,\beta\,m + \gamma}\,, \tag{42}$$

---

[1]) Si ha precisamente $\prod_{r,s}(y_r - y_s)^2 = 3125\,\nabla$.

Le formole (39), (41), (42) danno i valori di m, Z, n, che introdotti nelle (20) §. 121 esprimono le radici dell'equazione principale di 5.° grado per mezzo dell'irrazionalità icosaedrica. Riepiloghiamo i risultati ottenuti nel teorema:

L'equazione generale di 5.° grado si risolve con estrazioni di radici quadrate e coll'aggiunta di un'irrazionalità icosaedrica.

Ulteriori ricerche, che la natura del presente libro non ci consente di svolgere, sono relative alla così detta *risoluzione trascendente* dell'equazione dell'icosaedro, o dell'equazione di 5.° grado, per mezzo delle funzioni ellittiche (modulari). Si ottiene così un metodo di risoluzione dell'equazione generale di 5.° grado che dipende dalla divisione per 5 dei periodi delle funzioni ellittiche, analogamente come la risoluzione trigonometrica della equazione di 3.° grado si fa dipendere dalla trisezione dell'argomento delle funzioni circolari [1]).

[1]) Nel libro di KLEIN tante volte citato e nell'altra opera di KLEIN-FRICKE *Elliptische Modulfunctionem* il lettore troverà ampiamente svolto l'argomento.

INDICE

PARTE PRIMA

Teoria dei gruppi di sostituzioni.

Capitolo I.

Sostituzioni e loro composizione. — Gruppi di sostituzioni. — Gruppi transitivi ed intransitivi. — Gruppi imprimitivi e primitivi.

§. 1. — Sostituzioni e loro composizione . . . . . pag. 3
2. — Periodo di una sostituzione . . . . . » 6
3. — Sostituzioni circolari . . . . . » 8
4. — Trasposizioni e sostituzioni pari e dispari . . . . . » 10
5. — Sostituzioni trasformate e sostituzioni simili . . . . » 13
6. — Concetto di gruppo di sostituzioni o di operazioni . . » 14
7. — Teorema fondamentale . . . . . » 16
8. — Gruppo alterno come sottogruppo d'indice 2 . . . » 19
9. — Transitività ed intransitività dei gruppi . . . . . » 20
10. — Teoremi sui gruppi transitivi . . . . . » 22
11. — Limite superiore del grado di transitività . . . . . » 24
12-13. — Gruppi imprimitivi e primitivi . . . . . » 27

Capitolo II.

Isomorfismo dei gruppi. — Composizione e serie di composizione. — I teoremi di Sylow.

§. 14. — Isomorfismo oloedrico o meriedrico fra i gruppi . . . pag. 30
15. — Gruppi generali finiti di operazioni . . . . . » 33
16. — Sottogruppi invarianti. — Gruppi semplici e composti . . » 35
17. — Gruppo complementare di un gruppo rispetto ad un suo sottogruppo . . . . . » 36
18. — Teoremi fondamentali per la teoria della composizione. . » 39
19. — Fattori di composizione e teorema di Jordan. . . . . » 43
20. — Serie di composizione di gruppi isomorfi . . . . . » 45

§. 21. — Gruppi fattoriali e teorema di Hölder . . . . . pag. 47
22. — Serie di composizione principale . . . . . » 49
23-24. — Serie di composizione del gruppo totale . . . . . » 52
25. — Il primo teorema di Sylow . . . . . » 56
26. — Il secondo teorema di Sylow. . . . . » 61
27. — Gruppi di ordine p^r . . . . . » 64
28. — Gruppi semplici degli ordini da 1 a 100 . . . . . » 65
29. — Gruppi semplici d'ordine = 60 . . . . . » 68

Capitolo III.

Gruppi Abeliani. — Gruppo metaciclico. — Gruppo lineare totale e gruppo modulare.

§. 30-31. — Gruppi Abeliani e loro decomposizione in gruppi parziali . pag. 69
32-33. — Base di un gruppo Abeliano . . . . . » 73
34. — Invarianti dei gruppi Abeliani . . . . . » 76
35. — Gruppi transitivi risolubili sopra p elementi (p primo) . » 79
36. — Il gruppo metaciclico e le sue sostituzioni fondamentali S, T . » 80
37. — Rappresentazione analitica del gruppo metaciclico . . » 83
38. — Sottogruppi del gruppo metaciclico e serie di composizione . » 84
39. — Gruppo lineare totale sopra $p+1$ indici . . . . . » 87
40. — Periodo delle sostituzioni del gruppo lineare. . . . . » 90
41. — Sostituzioni generatrici del gruppo modulare . . . . » 92
42. — Semplicità del gruppo modulare per $p > 3$ . . . . . » 95

Capitolo IV.

Gruppi finiti di sostituzioni lineari sopra una variabile e loro rappresentazione geometrica come gruppi di rotazioni dei poliedri regolari.

§. 43. — Gruppi di sostituzioni lineari sopra una variabile . . pag. 99
44. — Poli delle sostituzioni di un gruppo finito . . . . . » 101
45. — Enumerazione dei possibili tipi di gruppi . . . . . » 104
46. — Gruppi ciclici e diedrali . . . . . » 105
47. — Gruppo del tetraedro . . . . . » 108
48. — Gruppo dell'ottaedro . . . . . » 110
49. — Gruppo dell'icosaedro . . . . . » 111
50. — La sfera complessa . . . . . » 115
51. — Formola di Cayley. . . . . » 116
52. — Movimenti di 2.ª specie . . . . . » 120
53. — Gruppi di rotazioni . . . . . » 121
54. — Le rotazioni del tetraedro e dell'ottaedro . . . . . » 123
55. — Le 60 rotazioni del gruppo dell'icosaedro . . . . . » 124
56. — Orientazione normale dei poliedri regolari . . . . . » 127
57. — Gruppi ampliati dei poliedri regolari . . . . . » 129

PARTE SECONDA

Teoria delle equazioni algebriche secondo Galois.

Capitolo V.

Irriducibilità delle equazioni. — Risolvente di Galois e gruppo di Galois per un'equazione. — Risolventi generali e loro gruppo. — Equazioni composte e loro riduzione a successive equazioni semplici.

§. 58. — Irriducibilità delle equazioni in un dato campo di razionalità pag. 135
59. — Teoremi relativi al campo assoluto di razionalità . . . » 137
60. — Esempi di equazioni irriducibili e procedimento di Kronecker . » 139
61. — Costruzione della risolvente di Galois . . . . . » 141
62. — Proprietà di questa risolvente . . . . . » 143
63 — Suo modo di decomposizione in fattori irriducibili. . . » 144
64. — Gruppo di Galois per una data equazione . . . . » 146
65. — Proprietà caratteristiche del gruppo di Galois . . . » 148
66. — Riduzione del gruppo di Galois per aggiunta di quantità . » 151
67. — Transitività od intransitività del gruppo di Galois . . » 153
68. — Equazioni che hanno per gruppo di Galois il gruppo totale . » ivi
69. — Formazione delle risolventi generali . . . . . » 156
70. — Gruppo di Galois della risolvente . . . . . » 159
71. — Equazioni a gruppo imprimitivo . . . . . » 160
72. — Equazioni composte ridotte a successive equazioni semplici . » 162

Capitolo VI.

Equazioni Abeliane. — Condizioni di risolubilità per radicali di un'equazione. — Risolventi di grado $< n$ dell'equazione generale di grado n. — Equazioni di grado primo risolubili. — Risolvente di Lagrange.

§. 73. — Equazioni Abeliane . . . . . pag. 164
74. — Risoluzione per radicali di un'equazione a gruppo ciclico . » 166
75. — Modificazione della formola di risoluzione . . . . . » 169
76. — Risoluzione di un'equazione Abeliana qualunque . . . » 172
77. — Caso delle equazioni Abeliane a coefficienti reali . . . » 173
78. — Equazione alle radici primitive p^{me} dell'unità . . . » 176
79. — Abbassamento del gruppo di un'equazione per la risoluzione completa di un'ausiliaria . . . . . » 178
80. — Teoremi sulla risolubilità di un'equazione per radicali . . » 181
81. — Insolubilità per radicali dell'equazione generale di grado $n < 4$ » 184
82. — Risolubilità parziale per radicali . . . . . » 186
83. — Aggiunta di una sola radice di un'ausiliaria . . . . » 187

§. 84. — Aggiunta di radicali reali e caso irriducibile dell'equazione cubica . . . . . pag. 189
85. — Impossibilità di risolventi di grado $< n$ dell'equazione generale di grado n . . . . . » 191
86. — Risolventi di grado n dell'equazione generale . . . . » 194
87. — Equazioni di grado primo risolubili . . . . . » 197
88. — Risolvente di Lagrange. . . . . » 199
89. — La risolvente di Lagrange per le equazioni di 5.° grado . » 200
90. — Equazioni metacicliche di 5.° grado . . . . . » 203

Capitolo VII.

Equazioni di Gauss per la divisione del circolo in parti eguali. — I periodi di Gauss e le successive risolventi. — Costruzione delle effettive formole di risoluzione mediante i numeri complessi $\psi_\mu(\alpha)$.

§. 91. — Equazioni per la divisione del circolo . . . . . pag. 205
92. — Equazioni $X_m(x)=0$ alle radici primitive m^{me} dell'unità . » 207
93. — Irriducibilità dei polinomii $X_m(x)$ secondo Kronecker . . » 209
94. — Gruppo Abeliano dell'equazione $X_n(x)=0$ . . . . . » 210
95. — I periodi η di Gauss per l'equazione $\frac{x^p-1}{x-1}=0$ . . . » 213
96. — La risolvente $F_e(\eta)=0$ ed il suo gruppo . . . . . » 216
97. — Risolventi successive dell'equazione $\frac{x^p-1}{x-1}=0$ . . . » 217
98. — I casi $p=5$, $p=17$ e i poligoni regolari di 5 e 17 lati . » 219
99. — La risolvente di 2.° grado per l'equazione $\frac{x^p-1}{x-1}=0$ . . » 222
100. — Il teorema di reciprocità nella teoria dei residui quadratici . » 225
101. — Le funzioni risolventi (ω^h, ε), (α^r, η_0) . . . . . » 226
102. — Formole fondamentali per le espressioni (ω^h, ε) . . . . » 228
103. — Formole di risoluzione per la $F_e(\eta)=0$ . . . . . » 230
104. — Decomposizione di un numero primo p in fattori complessi coniugati . . . . . » 232

Capitolo VIII.

Equazioni con un parametro e loro gruppo di monodromia. — Equazioni dei poliedri regolari. — Equazioni dell'icosaedro e sue risolventi di 5.° e 6.° grado. — Risoluzione della equazione generale di 5.° grado mediante l'aggiunta di un'irrazionalità icosaedrica.

§. 105. — Equazioni con un parametro e loro gruppo algebrico . . pag. 234
106. — Prima definizione del gruppo di monodromia . . . . » 235
107. — Il gruppo di monodromia come sottogruppo invariante del gruppo algebrico . . . . . » 236

§. 108. — Funzioni algebriche e loro punti critici . . . . pag. 238
109. — Nuova definizione del gruppo di monodromia . . . » 240
110. — Equazioni per la divisione dell'argomento delle funzioni circolari . . . . . » 241
111. — Equazioni dei poliedri regolari . . . . . » 244
112. — Costruzione di queste equazioni . . . . . » 246
113. — Loro gruppo di monodromia . . . . . » 247
114. — Sostituzioni omogenee del gruppo omogeneo icosaedrale G_{120} » 250
115. — Forme invarianti del gruppo omogeneo G_{120} . . . » 252
116. — Costruzione delle forme icosaedrali f, H, T . . . . » 255
117. — L'equazione dell'icosaedro . . . . . » 257
118. — Le risolventi dell'icosaedro e metodo invariantivo per la loro formazione . . . . . » 259
119. — Le forme ottaedrali t e W . . . . . » 261
120. — Le risolventi di 5.° grado delle u e delle r . . . . » 263
121. — La risolvente principale delle Y . . . . . » 265
122. — La risolvente di 6.° grado . . . . . » 268
123. — L'equazione principale di 5.° grado . . . . . » 271
124. — La sua risolvente di Galois icosaedrale . . . . » 273
125. — Risoluzione dell'equazione generale di 5.° grado mediante l'irrazionalità icosaedrica . . . . . » 276

CORREZIONE

Pag. 200, linea 9, manca l'intestazione del §. 89.